Universidade Católica Portuguesa
Faculdade de Engenharia

Segurança e Mobilidade em Redes IEEE 802.11

Modelo de suporte à decisão na escolha de arquitecturas e tecnologias de redes sem fios.

Daniel Maximino Caçador

Dissertação para obtenção do Grau de Mestre em Segurança em Sistemas de Informação

Júri

Prof. Doutor Manuel José Martinho Barata Marques (Presidente)
Prof. Doutor Rui Jorge Correia Mendes Alves Pires
Prof. Doutor Tito Lívio dos Santos Silva (Orientador)

Setembro de 2014

Universidade Católica Portuguesa
Faculdade de Engenharia

Segurança e Mobilidade em Redes IEEE 802.11

Modelo de suporte à decisão na escolha de arquitecturas e tecnologias de redes sem fios.

Daniel Maximino Caçador

Dissertação para obtenção do Grau de Mestre em Segurança em Sistemas de Informação

Júri

Prof. Doutor Manuel José Martinho Barata Marques (Presidente)
Prof. Doutor Rui Jorge Correia Mendes Alves Pires
Prof. Doutor Tito Lívio dos Santos Silva (Orientador)

Setembro de 2014

Resumo

A utilização de redes sem fios baseadas nas normas IEEE 802.11 é hoje em dia uma solução massificada [1] para comunicação de dados em ambientes diversificados, garantindo o acesso dos mais diversos tipos de dispositivos a plataformas de software, a aplicações e à Internet. A sua instalação em zonas públicas e instituições de grande dimensão implica a criação de infra-estruturas de acesso, a implementação de modelos de segurança e o dimensionamento adequado aos níveis de serviço pretendidos [2] para que se alcance a qualidade e fiabilidade exigida pelos utilizadores.

A crescente utilização de dispositivos móveis (*tablets, laptops, smartphones, etc.*) dentro e fora dos ambientes empresariais [3] apresenta desafios e preocupações de segurança que as empresas têm que considerar para disponibilizarem as suas aplicações de negócio com níveis de risco aceitáveis.

Nestes ambientes, os requisitos de segurança, desempenho e qualidade de serviço são especialmente relevantes, sobretudo quando estão envolvidas aplicações de negócio, onde a confidencialidade, integridade e privacidade da informação são aspectos críticos para as empresas num mundo cada vez mais competitivo.

Esta dissertação apresenta um estudo detalhado das especificidades deste tipo de redes ao nível físico, de controlo de acesso, ao nível da arquitectura, dos modelos de segurança, e aborda ainda as mais recentes evoluções da tecnologia tendo em vista a sua utilização em ambientes empresariais.

Para além de uma panorâmica dos problemas e soluções é proposta uma metodologia de suporte à decisão na escolha de arquitecturas, tecnologias e serviços de segurança, baseada num processo de segurança e num modelo de análise de risco que orientam o desenho arquitectural e os processos de implementação e operação para uma rede sem fios.

Palavras-chave: Sistema de informação, Ameaças, Vulnerabilidades, Segurança da informação, Redes sem fios, Mobilidade, Gestão de Risco.

Abstract

The use of wireless networks based on IEEE 802.11 standards are today a wide used solution [1] for data communication in diverse environments, ensuring access of all kinds of devices to software platforms, applications and Internet platforms. The installation on public areas and large institutions involves the creation of infrastructure for access, the implementation of security models and the correct dimensioning for the service level desired [2], in order to reach the quality and reliability required for the users.

The escalating use of mobile platforms (tablets, laptops and smartphones), inside and outside the corporate environments [3], represent new challenges and security concerns, which companies need to consider before making available their business applications with acceptable levels of risk.

In these environments, the security requirements, performance and quality of service are especially relevant when business applications are involved, mainly because confidentiality, integrity and privacy of information are critical aspects for companies in a competitive world.

This thesis presents a detailed study on the specificities of this type of networks at the physical level, access control, architecture, security models and also discusses the latest developments with a perspective of their use in business environments.

In addition to an overview of problems and solutions, we propose a methodology for decision support in the selection of architectures, technologies and security services, based on a security and a risk analysis process that guide the architectural design model, the implementation and operation processes to a wireless network.

Keywords: information system, threats, vulnerabilities, information security, wireless networks, mobility, risk management.

Agradecimentos

Ao meu orientado, o Prof. Doutor Tito Santos Silva, pela disponibilidade e conselhos recebidos de maneira a que o objectivo em vista fosse possível.

À minha família pelo apoio incondicional, compreensão nos momentos de maior indisponibilidade e por estarem sempre presentes.

Índice geral

Lista de tabelas

Lista de figuras

Lista de abreviaturas

Abreviatura	*Descrição*
ACK	Acknowledgment
AES	Advanced Encryption Standard
AP	Access Point
ARC	Adaptive Rate Control
BEB	Binary Exponential Backoff
bps	bits per second
BKM	Basic Key Management
CA	Certificate Authority
CBC	Cipher Block Chaining
CBC-CTR	Cipher Block Chaining Counter mode
CBC-MAC	Cipher Block Chaining Message Authenticity Check
CCMP	Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol
CHAP	Change-Handshake Authentication Protocol
CMDA	Code Division Multiple Access
CSMA	Carrier Sense Multiple Access
CRC-32	Cyclic Redundancy Check
CTS	Clear To Send
DCF	Distributed Coordination Function
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DoS	Denial of Service
DSL	Digital Subscriber Line
DSS	Digital Signature Standard
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
ESSID	Extended Service Set Identifier
FSK	Frequency Shift Keying
GHz	Gigahertz
GPS	Global Positioning System
http	Hypertext Transfer Protocol
IAPP	Inter Access Point Protocol
ICV	Integrity Check Value
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IV	Initialization Vector
KHz	Kilohertz

LAN	Local Area Network
Latência	Tempo decorrido entre o início de uma actividade e a sua conclusão.
LEAP	Lightweight EAP
MAC	Medium Access Control
Mbps	Megabits per second
MHz	Megahertz
MIC	Message Integrity Check
MIMO	Multiple-Input Multiple-Output
MSK	Master Session Key
OFDM	Orthogonal Frequency Division Multiplexing
Overhead	Custo adicional em processamento ou armazenamento
PAP	Password Authentication Protocol
PDA	Personal Digital Assistants
PEAP	Protected Extensible Authentication Protocol
PMK	Pair-wise Master Key
PRNG	Pseudo Random Number Generator
PSK	Phase Shift Keying
PTK	Pairwise Transient Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher 4
RSA	Rivest, Shamir and Adleman
RTS	Request To Send.
SIG	Special Interest Group
Spoofing	Imitação
SSID	Service Set Identifier
SYNK	Pacote de sincronismo
TA	Transmitter Address
TDMA	Time Division Multiple Access
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
TPC	Transmit Power Control
TTAK	Temporal and Transmitter Address Key
VOIP	Voice Over IP
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Networks
WMAN	Wireless Metropolitan Area Networks
WPA	Wi-fi Protected Access
WPAN	Wireless Personal Area Networks
WWiSE	World Wide Spectrum Efficiency
XOR	Exclusive OR

1. Introdução

A crescente utilização de redes sem fios, quer em ambiente empresarial [1], quer em ambiente público, veio trazer novos conceitos de mobilidade e conectividade e uma nova geração de novos serviços de valor acrescentado. A utilização de dispositivos móveis transformou os processos de comunicação pessoal e empresarial. Uma larga maioria de pessoas tem actualmente dispositivos com capacidade de voz, dados e Wi-Fi que lhe permitem ter presença contínua na internet, em redes sociais, acesso a correio electrónico, a vídeos e aplicações de negócio.

A riqueza de conteúdos, as exigências de desempenho das aplicações de negócio e a necessidade de mobilidade dos utilizadores, tem resposta nas várias normas internacionais de redes sem fios que têm ficado disponíveis na última década e que constituem já uma alternativa às redes convencionais, seja porque se se tornaram uma alternativa economicamente viável, seja pela sua capacidade de fornecerem taxas de transmissão comparáveis às das redes cabladas.

1.1. Motivação

A crescente utilização de redes sem fios, especialmente as redes IEEE 802.11, em redes de acessos público e privado, exige aos operadores a capacidade de fornecer comunicações seguras. A segurança estende-se aos domínios da privacidade, confidencialidade e integridade dos dados transmitidos, bem como aos serviços de autenticação das entidades intervenientes.

Dadas as características físicas do meio de comunicação de rádio utilizado, as redes sem fios devem possuir requisitos de segurança mais exigentes do que as redes convencionais cabladas. Para além dos riscos existentes nas redes cabladas, nas redes sem fios acrescentam-se novos riscos pelo facto de a transmissão ser efectuada por radiofrequência, onde se torna possível a intercepção, personificação ou negação de serviço.

Das diversas normas para redes sem fios utilizadas, tais como IrDA, Bluetooth, HiperLan, Wi-Fi e Wi-Max, a norma IEEE 802.11 Wireless LAN (a/b/g/n/ac) é actualmente a solução de redes sem fios de baixo custo mais difundida em todo o mundo.

As várias gerações de normas IEEE 802.11, iniciadas na norma 802.11 original até à actual quinta geração com a norma 802.11ac [2] apresentaram melhorias tanto em termos de desempenho (Figura 1-1) como em termos de mecanismos de segurança (Figura 5-1).

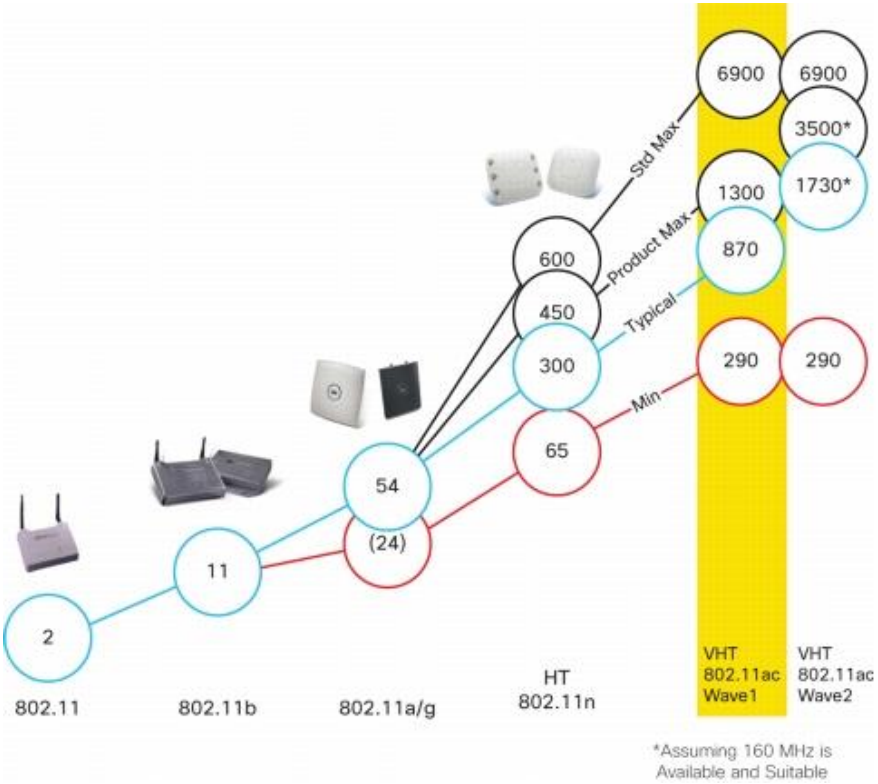

Figura 1-1: Evolução do nível físico das redes IEEE 802.11 [3]

Na sua versão inicial, definida em 1997, o IEEE 802.11 suportava velocidades até 2 Mbps usando frequências de rádio livres de licenciamento. Através da evolução da norma em 1999 ficaram disponíveis velocidades de transmissão mais elevadas, como sejam os 11Mbps na norma IEEE 802.11b e 54 Mbps na norma IEEE 802.11a. Em 2003 foi ratificado a norma IEEE 802.11g que funciona na banda dos 2,4 GHz, permitindo velocidades de 54Mbps. Com o aumento da procura de aplicações de tempo real sobre rede sem fios, iniciou-se um novo grupo de trabalho IEEE 802.11n em 2002, cuja norma foi ratificado em 2009, para a especificação de um novo MAC (*Medium Access Control*) e um novo meio físico, que permitisse aumento de velocidades até um máximo de 600 Mbps [4]. Actualmente a nova norma de rede sem fios, IEEE 802.11ac, publicada em Dezembro de 2013, permitir aumentar as velocidades de transmissão até 6,93 Gbps.

Em face desta realidade, e da crescente proliferação de dispositivos com acesso a redes sem fios, o estudo das várias normas 802.11 e dos mecanismos de segurança disponíveis actualmente adoptados em redes não-cabladas IEEE 802.11 são o tema principal desta dissertação.

1.2. Objectivos

Esta dissertação tem como principal objectivo o estudo das diversas tecnologias e dos protocolos de segurança das redes sem fios e apresentar uma metodologia que permita a implementação de redes sem fios, baseada num modelo de análise de risco, bem como os processos de monitorização e melhoria inerentes à sua utilização.

Em particular, descrevem-se os seguintes objectivos específicos:

- O estudo detalhado dos protocolos, tecnologias e arquitecturas de redes sem fios, ao nível dos modelos de arquitectura, de segurança e risco;
- O estudo dos mecanismos de segurança implementados pela norma IEEE 802.11.
- Avaliar as principais ameaças à segurança nas redes sem fios;
- Compreender o funcionamento dos diferentes mecanismos de segurança, estudar as suas vulnerabilidades e possíveis ataques;
- Identificar os indicadores mais relevantes na escolha dos modelos de arquitectura e segurança;
- Identificar modelos de arquitectura e segurança que suportem as necessidades de mobilidade, desempenho e de qualidade de serviço tendo em vista a sua utilização em ambientes empresariais;
- Propor um modelo de suporte a tomadas de decisão relativamente à escolha da arquitectura das redes sem fios, dos modelos de segurança e das tecnologias envolvidas;

1.3. Estrutura

Esta dissertação encontra-se estruturada em 8 capítulos, organizados da seguinte forma.

No capítulo 2 é efectuado um estudo relativo às ameaças e à tipificação dos ataques que poderão ser efectuados nas redes sem fios. A compreensão das vulnerabilidades nas redes sem fios irá permitir avaliar os mecanismos e protocolos de segurança mais adequados à protecção das redes.

No capítulo 3 introduzem-se os conceitos básicos de segurança. São apresentados os princípios de criptografia, a criptografia de chave secreta e chave pública, os serviços de autenticação, confidencialidade, integridade e não-repúdio. São também apresentadas as funções de síntese, gestão e distribuição de chaves criptográficas e certificação digital. Estes conceitos permitem a compreensão dos algoritmos criptográficos disponibilizados nos protocolos de segurança das redes sem fios.

No capítulo 4 apresentam-se as tecnologias e modo de funcionamento das redes sem fios associadas à norma IEEE 802.11 e as diversas topologias e modos de funcionamento.

No capítulo 5 estudam-se os protocolos de segurança utilizados em redes sem fios. São apresentados os serviços de autenticação, confidencialidade e integridade. Descreve-se o protocolo WEP e o IEEE 802.11i. Apresenta-se também o protocolo de autenticação 802.1X integrado nas variantes LEAP, EAP-TLS, EAP-TTLS e PEAP.

No capítulo 6 são apresentadas as vulnerabilidades do protocolo WEP e a evolução dos protocolos de segurança.

No capítulo 7 é apresentada uma proposta de metodologia para a segurança de redes sem fios. Apresenta-se um processo que permite, de uma forma sistemática, desenhar uma solução arquitectural e processual para a implementação e operação de uma rede sem fios. Tem como diferenciador a utilização do processo de análise de risco, baseado na ISO 27005.

Esta dissertação termina no capítulo 8, onde se apresentam as principais conclusões do trabalho realizado e tópicos para trabalho futuro.

2. Ameaças às redes sem fios

O aparecimento das normas de redes sem fios baseadas na utilização de frequências não licenciadas proporcionou o grande crescimento e a utilização de dispositivos móveis em face dos benefícios que advêm da utilização desta tecnologia, bem como dos reduzidos custos necessário para a implementar e da facilidade da sua instalação.

Um desafio fundamental na garantia da segurança da tecnologia de redes sem fios é o facto de não haver segurança física para o seu acesso. Com as redes sem fios, perde-se a capacidade de limitar o acesso a recursos internos de uma organização através do controlo do acesso físico à mesma. Desta forna, verifica-se que os ataques [5] associados às redes sem fios utilizam métodos diferentes dos utilizados nas LANs.

Outro aspecto a considerar nas redes em fios é o novo risco associado ao facto de ter utilizadores ligados à rede sem estarem validados e/ou autorizados. Os utilizadores poderão potencialmente ligar-se a qualquer rede ao seu alcance, mesmo a redes às quais não têm permissão, através de mecanismos de "associação", podendo esse utilizador ser um atacante com o objectivo de explorar uma determinada rede ou sistema.

O paradigma de controlo de acesso também é diferente nas redes sem fios. Tradicionalmente os administradores protegem as redes de acessos não autorizados. No entanto, o paradigma muda, sendo necessário não só proteger as redes sem fios de acesso não autorizado, mas também proteger os utilizadores de uma organização de se ligarem a redes às quais não deverão ter acesso.

A segurança das redes sem fios é um desafio para os administradores das redes e de segurança da informação. Ao contrário das redes de cabo LAN (Ethernet), as redes sem fios IEEE 802.11, emitem o seu sinal de radiofrequência para todos os clientes que possam "ouvir". Como consequência, qualquer um com as ferramentas adequadas pode capturar e transmitir sinais de radiofrequência se estiver dentro do seu alcance.

A protecção de uma rede depende dos riscos identificados sobre os diversos activos de informação que por ela circulam. A importância dos dados a proteger, o impacto originado pela sua perda ou pela divulgação de informação confidencial, irá definir os requisitos de protecção a implementar. Para garantir a segurança numa rede é importante compreender quem a poderá

atacar, qual a forma, ferramentas e técnicas utilizadas para desencadear os ataques [5]. A identificação destes aspectos, enquadrada numa metodologia que se irá apresentar, permitirá conceber um plano de segurança que defina quais os controlos a serem implementados – desenho arquitectural, serviços disponíveis na rede e tipo de acessos permitidos. Face às características próprias das redes sem fios, é importante o estudo das ameaças a este tipo de rede, possibilitando desta forma desenvolver uma análise de risco que permita, posteriormente, a escolha dos controlos mais ajustados.

Este capítulo descreve na secção 2.1 o tipo de entidades que poderão atacar as redes sem fios. Na secção 2.2 apresenta-se um conjunto de ameaças e ataques às redes sem fios e, quando possível, quais as ferramentas que poderão se utilizadas.

2.1. Tipo de atacantes

O conhecimento de quais os potenciais inimigos ou intrusos e as suas motivações é importante para a definição dos mecanismos de protecção de uma rede sem fios. Serão estes que, através da utilização de um conjunto de ferramentas de *software* e/ou *hardware*, tentarão desenvolver ataques à rede sem fios. Poderá ser considerado como intruso qualquer utilizador não autorizado, que usa todos os meios ao seu alcance para obter informação e acesso a recursos apenas disponíveis a utilizadores autorizados.
Numa perspectiva de segurança os utilizadores não autorizados podem ser divididos nas seguintes categorias:

- **Utilizadores acidentais** – Utilizadores que não tentam aceder de forma intencional à rede e que podem, inclusive, não saber que a rede existe ou que tiveram acesso a ela. Se os dispositivos móveis ou computadores destes utilizadores estiverem configurados para efectuarem associações a qualquer rede de forma automática, logo que esta seja detectada, estes poderão obter acesso a recursos de uma rede de forma não intencional. Esta situação é comum em *hot spot*s públicos.
- **Intrusos amadores** – Utilizadores como poucos conhecimentos técnicos, que têm intenção de aceder de forma não autorizada. Utiliza normalmente ferramentas públicas descarregadas da internet para desenvolver o seu ataque. É expectável algum sucesso apenas em redes com poucas ou nenhumas medidas de segurança.
- **Intrusos profissionais** – Utilizadores com elevado nível de conhecimentos e perícia, que por interesses financeiros ou motivos profissionais, desenvolvem

ataques utilizando ferramentas [5] e técnicas de intrusão, exploram vulnerabilidades e fraquezas da rede, permitindo o acesso a informação ou serviços de forma não autorizada.

No desenvolvimento do processo de segurança das redes sem fios (7.1), nomeadamente na fase de análise de risco, deverá ter-se em atenção o tipo de atacantes que poderão desencadear os ataques, influenciando desta forma a probabilidade da exploração de vulnerabilidades.

2.2. Ameaças e ataques à segurança de redes sem fios

A protecção de uma rede deverá ser assegurada por um conjunto de serviços de segurança (3.1.1) dos quais se destacam a autenticação, confidencialidade, integridade, disponibilidade e não-repúdio.

Existem vários tipos de ameaças, cada uma afectando um ou mais serviços de segurança e que se concretizam através de ataques à confidencialidade e integridade dos dados, ou à disponibilidade da rede e de ataques de personificação.

Normalmente os métodos de ataques podem ser classificados como Activos ou Passivos.

- **Ataque passivo** - consiste num acesso não autorizado, sem conhecimento dos interlocutores ou donos, a um activo ou rede com o objectivo de captura ou análise de tráfego, mas não modificando o seu conteúdo. Este ataque é de difícil detecção porque os dados não são modificados. Consequentemente deverá dar-se ênfase à prevenção através de técnicas de cifra dos dados.
- **Ataques activos** - consistem num acesso não autorizado, sem conhecimento dos interlocutores ou donos, a um activo ou rede com o objectivo de modificação dos dados (ex: mensagem, ficheiro) ou de criação de disrupção nos serviços de rede (DoS).

O diagrama (Figura 2-1) seguinte apresenta uma taxonomia de ataques a redes sem fios

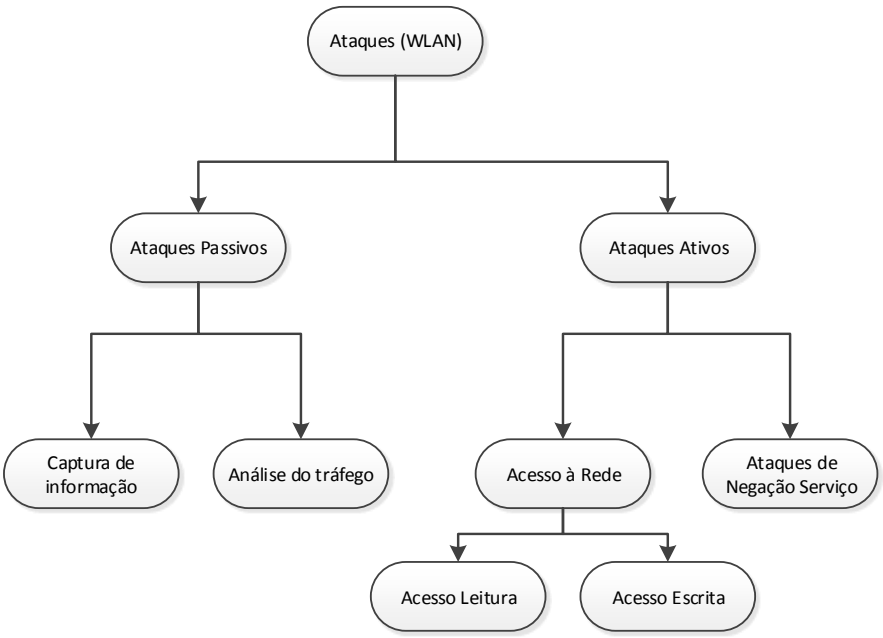

Figura 2-1: Taxonomia de ataques de segurança a redes sem fios [6]

2.2.1. Ataques passivos

Os **ataques passivos** são efectuados com o objectivo de recolher dados em trânsito, sem interrupção das comunicações, entrando na rede através de uma falha de segurança.

Existem normalmente duas fases num ataque. A primeira fase conhecida como **reconhecimento** corresponde a um ataque passivo. Durante a fase de reconhecimento, o objectivo de um atacante é a descoberta de uma rede alvo e então obter toda a informação possível da mesma. O atacante executa estas actividades de uma forma indetectável, não revelando a sua presença. No entanto, alguns métodos de reconhecimento poderão ser detectados por sistemas de detecção de intrusão (IDS).

Existem dois métodos típicos de execução de ataques passivos:

- **Captura de informação**: Através da monitorização e escuta de um meio de transmissão, pode capturar-se as mensagens que circulam de forma indetectável. A captura de informação poderá ser efectuada através das seguintes técnicas:
    - **AP intrusos:** Quando se utiliza um processo de chaves partilhadas não existe autenticação mútua entre os AP e as estações.
    - **Escuta do meio Radio Frequência RF:** Um modo comum de ataque é colocar uma estação a capturar a comunicação de Rádio Frequência que ultrapassa as

paredes das instituições. Se houver pouca segurança facilmente se obtêm as mensagens, se o canal transmitir em claro ou se forem descobertas as chaves de cifra, podendo desta forma aceder ilicitamente à rede.

- **Análise de tráfego**: com os dados obtidos por captura de informação poderá ser possível desenvolver análise da mesma, com vista à obtenção de dados em claro (no caso da informação estar cifrada) ou de chaves criptográficas.

Estão disponíveis na internet imensas ferramentas de escuta (*sniffing*) que podem ajudar um atacante a atingir o seu objectivo. As ferramentas de escuta são os meias mais eficazes de monitorização do que está a ocorrer numa rede. São indetectáveis e permitem duas funções principais: captura de pacotes e análise e apresentação dos pacotes. Através da análise dos pacotes, um atacante fica informado das características da rede, e pode obter diversas informações confidenciais para usar contra uma organização. A captura de pacotes permite a um atacantes calcular chaves WEP numa questão de minutos, possibilitando desta forma ler e capturar todos os dados que transitam entre estações e os APs.

Outra técnica utilizada para reconhecimento é conhecida como "*War Driving*", e consiste no acto de ir identificando as redes sem fios IEEE 802.11 e respectivos protocolos de segurança, que se encontram ao alcance de um receptor enquanto se percorre uma rua ou cidade. Se a estas redes identificadas forem associadas as suas coordenadas GPS e disponibilizada a informação num *site* publico na internet, aumenta consideravelmente o risco de ataques.

Entre as diversas ferramentas de escuta, encontram-se várias gratuitas, como sejam o "*Wireshark*", *NetStumbler/Vistumbler* (Windows), *kismet* ou *SWScanner* (Linux), *KisMac* (Macintosh). Na Tabela 2-1 estão identificadas algumas das ferramentas [5] mais populares.

Tabela 2-1: Ferramentas para ataques passivos

Ferramenta	Capacidades	Origem	Notas
Wireshark v1.10.6 Abril/2014	Detecção de redes sem fios, escuta, recolha de pacotes	http://www.wireshark.org/	Recolha passiva Bom interface gráfico Analisador de protocolos
Tcpdump V4.5.1 Jan/2014	Detecção de redes sem fios, escuta, recolha de pacotes	http://www.tcpdump.org/	Recolha passiva
Kismet 2013-03-R1b Abril/2013	Detecção de redes sem fios, escuta, recolha de pacotes	http://www.kismetwireless.net/	Recolha passiva
KisMac v0.3.3 Fev/2011	Detecção de redes sem fios, escuta, recolha de pacotes	http://kismac-ng.org/	
NetStumbler V0.4.0 Abril 2004	Detecção de redes sem fios	http://www.stumbler.net/	
Vistumbler v10.5 Agosto 2013	Detecção de redes sem fios	http://www.vistumbler.net/	
Microsoft Network Monitor V3.4 Junho 2010	Detecção de redes sem fios, escuta, recolha de pacotes	http://www.microsoft.com/en-us/download/details.aspx?id=4865	
Message Analyser V 1.0 Setembro/2013	Detecção de redes sem fios, escuta, recolha de pacotes	http://www.microsoft.com/en-us/download/details.aspx?id=40308	
Aircrack-ng v 1.2 Beta 3 Março 2014	Descoberta de chaves WEP e WPA-PSK	http://www.aircrack-ng.org/	

2.2.2. Ataques activos

Um ataque activo é aquele onde é tentada uma alteração não autorizada num sistema. Isto pode incluir, por exemplo, a modificação de dados transmitidos ou guardados, a criação de novos fluxos de dados, a limitação ou interrupção da actividade de rede de uma organização. Ataques activos podem ser classificados nas seguintes categorias: personificação (*masquerading*),

homem-no-meio (*man-in-the-middle*), modificação de mensagens e negação de serviço (*denial-of-service - DoS*).

2.2.2.1. Personificação (*Masquerading*)

Este ataque acontece quando um atacante assume a identidade de um utilizador autorizado e consegue obter certos privilégios sem autorização. Pode ser tentado através da utilização de identificadores e palavras-chaves, através de falhas de segurança em programas ou através da ultrapassagem dos mecanismos de autenticação. A tentativa pode provir de um elemento interno da rede (um empregado como exemplo) ou de um elemento externo, através de uma rede pública.
Esta é a aproximação ideal quando um atacante se quer manter indetectável. Se um determinado utilizador ou dispositivo consegue fazer-se passar por outro, o atacante obtém todos os acessos estabelecidos durante a entrada na rede, não sendo possível detectá-lo a não ser que efectue acções anormais, como seja aceder a áreas de sistema.

2.2.2.2. Homem no meio (*Man-in-the-Middle – MITH*)

Este ataque também é conhecido por ataque de retransmissão (*replay*) e corresponde à situação onde um atacante se coloca entre uma estação (fazendo-se passar por um AP autorizado) e um AP (fazendo-se passar por uma estação autorizada), capturando o tráfico e podendo em algumas situações capturar, alterar ou duplicar os dados antes de os enviar, de forma a que sejam executadas operações não autorizadas ou ilegítimas.

Este tipo de ataque é possível mediante a utilização de um processo denominado *Address Resolution Protocol (ARP) spoofing*. Este processo é efectuado da seguinte forma: o ARP identifica o endereço *Medium Access Control* (MAC) para um determinado endereço IP. Sempre que um dispositivo pretende comunicar com o seu par numa rede IP, envia um pedido ARP por difusão na rede solicitando o endereço MAC do IP do interlocutor. Um atacante poderá responder com o endereço MAC do seu dispositivo que identifica o endereço IP do pedido. A partir desse momento, todas as comunicações entre os dispositivos são primeiro encaminhadas para o dispositivo do atacante, permitindo a recolha, manipulação ou eliminação da informação. Exemplo das ferramentas que permitem realizar este tipo de ataques são o *ettercap* e o *Caim e Abel*.

2.2.2.3. Modificação de mensagem

A modificação de mensagens poderá ser efectuada através da alteração, supressão, ou criação de dados de mensagens ou mesmo da alteração da sua ordem de transmissão. Como exemplo, se houver a intercepção de mensagens numa rede sem fios e se houver alteração do IP destino das mensagens, o tráfico poderá ser encaminhado para um dispositivo na LAN ou na Internet. Como o cabeçalho IP é fácil de atacar, e o tráfico é decifrado nos AP, a mensagens será interceptada a claro.

2.2.2.4. Negação de serviço (*Denial of Service - DoS*)

Este ataque tem como objectivo reduzir ou interromper a comunicação na rede. Os ataques de negação de serviço poderão ser alcançados através da destruição física dos equipamentos, ou da disrupção de certos serviços ou sistemas, através do empastelamento da rede, impossibilitando o tráfego legítimo na rede. Existem algumas formas de desenvolvimento destes ataques:

- Utilização de um equipamento de empastelamento das frequências de rádio
- Saturar a largura de banda da rede através do envio contínuo de tramas.
- Efectuar ataques de dissociação/desautenticação
- Saturar as tabelas de associação dos APs

Para se conseguir um ataque activo, um atacante necessita de ter um acesso de escrita e leitura à rede a atacar. O objectivo principal é obter acesso aos recursos da rede ou capturar e decifrar os dados que circulam na mesma. O acesso de leitura permite a um atacante interceptar e ler tráfego da rede, possibilitando-lhe a capacidade de efectuar ataques à cifra, autenticação e outros métodos de protecção. Após a descoberta de uma rede através de mecanismos de reconhecimento, e de ter capturado tráfego a claro e cifrado através do método de *sniffing*, um atacante tem a possibilidade de obter informação que lhe possa permitir a recuperação de chaves criptográficas.

A obtenção das chaves criptográficas permitirá ao atacante um acesso sem restrições à rede a atacar, podendo desta forma fazer o envio de tráfego para qualquer elemento da rede.

Um atacante poderá ter diversos objectivos para atacar uma rede, como sejam:

- Obtenção de chaves de cifra;
- Obtenção da informação de fluxos de dados cifrados com as chaves de cifra;

- Injecção de pacotes de dados em claro ou cifrados através do reenvio de pacotes capturados;
- Cifrar dados com chaves capturadas e a sua injecção na rede;
- Instalação de *software* de captura de dados ou código malicioso em clientes de redes sem fios;
- Configuração de um AP falso com a mesma identificação (*rouge AP*) para captura de informação dos clientes;
- Ultrapassar os esquemas de autenticação:
    - Através de falsificação dos endereços MAC (*MAC spoofing*) para ultrapassar filtros de controlo utilizando endereços MAC.
    - Através de ataques a chaves partilhadas;
    - Através de ataques de dicionário, se as redes utilizarem mecanismos 802.1X para autenticação;

As redes sem fios IEEE 802.11 têm na sua génese problemas de segurança na sua arquitectura, começando logo pela necessidade de os AP e os clientes necessitarem de se anunciar (trama "*beacon*"). Desta forma fica exposto um sinal para quem esteja no seu alcance e tenha capacidade de o escutar. Criar um escudo numa rede sem fios, através da escolha de uma localização que não permita que os sinais de RF sejam emitidos para fora das áreas reservadas, irá reduzir os riscos dos acessos não autorizados. No entanto, esta solução nem sempre é viável. Como consequência deverão ser implementados outros métodos de segurança, como sejam tecnologias de cifra e controlo de acessos.

As técnicas para obter acessos não autorizados nas primeiras normas de redes sem fios foram muito divulgadas e tiveram como resultados o desenvolvimento da norma IEEE 802.11i. Apresentam-se de seguida os diversos ataques às redes sem fios, agrupados por categorias.

2.2.2.5. Ataques a controlo de acessos

Estes ataques tentam penetrar numa rede, ultrapassando filtros ou *firewalls* para obter o acesso à rede (Tabela 2-2). Os ataques mais comuns consistem em técnicas de *MAC Spoofing* e de *Rogue AP* logo após a "escuta" do meio RF para obtenção da informação necessária (endereços MAC ou SSID).

Tabela 2-2: Ataques a controlo de acessos

Ataque	Descrição	Métodos e ferramentas [5]
"War driving"	Descoberta de redes sem fios através da escuta das tramas "*beacon*" ou através de envio de tramas "*probe request*" para obtenção de informação para ataques.	DStumbler, KisMAC, MacStumbler, NetStumbler, WaveStumbler,
Rogue AP	Instalação de um AP falso dentro da rede interna da entidade, criando uma porta aberta para a rede interna.	Qualquer *hardware* ou *software*
MAC spoofing	Reconfiguração do endereço MAC do atacante igual ao de uma estação fidedigna e autorizada na rede ou de um AP.	Qualquer placa de rede sem fios
Quebra de segurança no acesso através de 802.1X.	Obtenção de chaves de acesso através de ataques de força bruta utilizando pedidos de acesso 802.1X.	Ferramentas de captura de pacotes entre AP e servidor de RADIUS

2.2.2.6. Ataques à integridade

Estes ataques consistem no envio de tramas falsificadas de gestão, controlo ou de dados para a rede sem fios, possibilitando dessa forma adulterar as comunicações de clientes ou inviabilizar o seu acesso. Ataques de negação de serviço são um dos exemplos mais comuns deste tipo de ataques (Tabela 2-3).

Tabela 2-3: Ataques à integridade

Ataque	Descrição	Métodos e ferramentas [5]
Injecção de tramas 802.11	Envio de tramas 802.11 falsificadas ou adulteradas	
Injecção de tramas de dados duplicadas 802.11	Captura e reenvio de tramas de dados 802.11 (com ou sem adulteração)	
Eliminação de tramas de dados 802.11	Através de empastelamento de sinal RF corromper as tramas de dados, e simultaneamente enviando as tramas de ACK correspondentes.	

Reenvio de tramas 802.1X EAP	Captura de tramas 802.1X EAP ("*Identity*", "*Success*", "*Failure*") para reemissão futura.	
Reenvio de tramas 802.1X RADIUS	Captura de tramas 802.1X "Access", ("Accept" ou "Reject") para reemissão futura.	

2.2.2.7. Ataques à confidencialidade

Estes ataques tentam interceptar informação privada ou sensível enviada através da rede sem fios que esteja em claro ou cifrada (Tabela 2-4).

Tabela 2-4: Ataques à confidencialidade

Ataque	Descrição	Métodos e ferramentas [5]
Escuta	Captura e descodificação do tráfego de rede para obtenção de informação sensível	Ettercap, kimnet, wireshark
Quebra de chaves WEP	Captura de pacotes para recuperar chaves WEP utilizando o método de força bruta ou criptoanálise *Fluher-Mantin-Shamir* (FMS)	Aircrack, airsnort
AP falso	Colocar um AP falso anunciando SSID iguais aos AP verdadeiros para obter informações.	HostAP, HermesAP
AP Phishing	Execução de portal num AP falso com objectivo de obter credenciais de utilizador.	Airsnaf
Man-in-the Middle	Ataques descritos anteriormente	Dsniff, ettercap, Ccaim Abel

2.2.2.8. Ataques à autenticação

Estes ataques são usados para obtenção ilegítima da identidade e credenciais de acesso à rede ou a serviços disponibilizados (Tabela 2-5). Ataques de dicionário ou de força bruta são as duas técnicas mais comuns para executar este ataque. Em caso de sucesso o atacante pode personificar um utilizador autorizado e obter acessos ilegítimos.

Tabela 2-5: Ataques à autenticação

Ataque	Descrição	Métodos e ferramentas [5]
Calcular a Chave secreta	Tentativa de adivinhar a chave secreta	Ferramentas para quebras de chaves WEP.
Quebra de chaves PSK	Recuperação da chave WPA PSK através de tramas capturadas durante o processo de autorização utilizando ataques de dicionário	Wpa_crack,
Roubo de credenciais de acesso a aplicações	Captura de credenciais de utilizadores	WinSniffer, Ace Password Sniffer, Dsniff
Roubo de credenciais de domínio	Recuperação de credenciais de utilizadores (ex: login Windows e palavra chave) através da quebras dos *hash* da *password NetBIOS*.	Cain Abel, L0phtCrack

3. Conceitos fundamentais de segurança em redes

Para uma protecção efectiva de uma rede torna-se necessário garantir a protecção dos dados sensíveis que nela circulam, das aplicações e dos recursos disponibilizados. A implementação de mecanismos criptográficos vem possibilitar a implementação de serviços de confidencialidade, integridade, não repúdio. A definição dos mecanismos de segurança que implementam estes serviços é função da política de segurança a definir para a rede. A utilização de determinados mecanismos exige mais processamento nos diversos componentes da rede, no entanto para situações onde a segurança é importante, a perda de desempenho é compensado pela redução dos riscos obtida.

Para uma melhor compreensão dos mecanismos de segurança que foram introduzidos ao longo do tempo nas normas de redes sem fios, torna-se importante descrever os conceitos fundamentais de serviços de segurança e os mecanismos de criptografia.

Este capítulo começa por introduzir os conceitos de serviços de segurança na secção 3.1. Na secção 3.2 apresenta-se uma categorização das medidas de segurança, seguindo-se uma descrição dos conceitos de criptografia na secção 3.3. Na secção 3.4 é apresentado o funcionamento das cifras modernas, como sejam as chaves simétricas utilizada nos algoritmos *Rivest Code 4* (RC4) e *Advanced Encryption, Standard* (AES), as chaves assimétricas utilizadas nos algoritmos *Rivest Shamir Addleman* (RSA) e *Diffie-Hellman* (DHE) e funções de síntese utilizadas nos algoritmos *Message Digest 5* (MD5) e *Secure Hash Algorithm* (SHA-1), que estão na base dos mecanismos de segurança das redes sem fios descritos na secção 5.

3.1. Conceitos

A segurança em redes de comunicações não deve ser vista como a segurança de cada uma das suas componentes isoladas mas sim como algo que tem uma abrangência maior em termos de políticas, serviços e mecanismos de segurança. Os objectivos de segurança fundamentais nas redes: confidencialidade, integridade e disponibilidade, irão ser assegurados através da implementação conjugada de políticas e mecanismos de segurança.

Para se compreender como pode ser implementada a segurança em redes de comunicações apresentam-se os seguintes conceitos elementares [59]

- **Políticas de segurança** – São constituídas por um conjunto de regras, mais ou menos complexas, aplicadas a procedimentos e actividades relacionadas com as necessidades administrativas e de gestão de recursos (ex: rede de comunicações) à qual se aplicam.
- **Autorização** – Acção que atribui os direitos de acesso de uma entidade a um recurso. Está normalmente integrada numa determinada politica de segurança que dita quem pode fazer o quê e a que recursos.
- **Ameaça** – Identifica a entidade, pessoa ou evento que constitui algum risco. Este risco pode estar relacionado com a exploração de uma vulnerabilidade num dos objectivos de segurança fundamentais: confidencialidade, integridade e disponibilidade.
- **Ataque** – É a concretização de uma determinada ameaça. Um ataque pode ser classificado como activo ou passivo. Um exemplo deste último é a "escuta" não autorizada ou *sniffing* de uma rede de comunicações, com o intuito de obter dados.
- **Risco** - É o potencial de uma determinada ameaça de explorar vulnerabilidades de um activo ou de um conjunto de activos e de causar danos numa organização [7] (*ISO 27005*). O risco é proporcional ao valor dos dados ou activos e à probabilidade de um ataque ser bem-sucedido.
- **Medidas de protecção** – Conjunto de políticas de segurança, mecanismos de controlo de acesso, procedimentos de monitorização e de resposta, que diminuem a possibilidade de ocorrência de um ataque bem sucedido. Entre as medidas de protecção que devem ser implementadas destacam-se os mecanismos de autenticação, confidencialidade e de integridade.

3.1.1. Serviços de segurança

Os serviços de segurança dizem respeito a conceitos de segurança que poderão ser implementados através de mecanismos que incluem um conjunto de ferramentas criptográficas. A norma X.800 define os serviços de segurança [8] como:

- **Confidencialidade** - A propriedade de que a informação não fique disponível ou seja divulgada a pessoas, processos ou entidades não autorizados.
- **Integridade** - A propriedade de que os dados (ou informação) não foram alterados ou destruídos de uma forma não autorizada.
- **Disponibilidade** - A propriedade de estar disponível e utilizável mesmo em carga por uma entidade autorizada.

- **Controlo de acesso** - A prevenção do uso não autorizado de um recurso, incluindo a prevenção do uso do recurso para fins não autorizados.
- **Autenticação da origem dos dados** - A comprovação de que a fonte dos dados recebidos é conforme o indicado.
- **Autenticação de entidades de uma associação** - A comprovação de que uma entidade numa associação entre entidades é a que é indicada. Existe uma distinção clara entre "identificação" e "autenticação". Identificação refere-se a uma entidade (utilizador, equipamento) que alega a sua identidade fornecendo um identificador (nome, endereço de email, endereço IP, nome de domínio, etc), ou o procedimento de encontrar a identidade de um utilizador entre *N* utilizadores conhecidos pelos sistemas sobre vários aspectos. Autenticação consiste em provar a identificação fornecida, fornecendo um ou vários elementos de autenticação (chaves de acesso, *tokens hardware*, *smart-cards,* etc).
- **Detecção de reprodução** - A detecção de reprodução consiste na capacidade de uma entidade detectar que os dados recebidos são duplicados relativamente a outros recebidos anteriormente. Mesmo que os dados tenham sido transmitidos por canais seguros de uma entidade legítima, é possível que sejam copiados e "injectados" de novo para o mesmo destinatário. Apesar dos dados serem autênticos é necessário detectar a repetição dos mesmos e evitar que sejam processados mais que uma vez.
- **Não repúdio** – Garantir que uma das partes envolvidas na comunicação possa, indevidamente, negar que esta mesma comunicação ou a informação transmitida, alguma vez tenha ocorrido.

Os mecanismos de cifra possibilitam a implementação dos serviços de confidencialidade. Os serviços de integridade e de autenticação da origem são muitas vezes implementados através dos mesmos mecanismos de segurança: funções de síntese e geradores MAC (Message Authentication Code). Os mecanismos de detecção de reprodução baseiam-se na introdução de um número de sequência a cada elemento transmitido.

A razão da implementação dos serviços de segurança é por isso de proteger a informação de uma organização enquanto a torna disponível a quem está autorizado a usá-la. Os atacantes tentam normalmente prejudicar um sistema ou perturbar o seu normal funcionamento, explorando as vulnerabilidades dos mesmos através do recurso a várias técnicas, métodos e ferramentas [5]. Os administradores e gestores de redes precisam de perceber os vários aspectos de segurança a ter em conta, para que as políticas e os procedimentos de segurança sejam definidos adequadamente.

3.2. Medidas de protecção e ameaças à segurança

A segurança das redes deve prevenir e detectar acções não autorizadas levadas a cabo por utilizadores ilegítimos, com vista à protecção da informação que circula nas mesmas. Este conceito de segurança é mais abrangente e inclui outros aspectos, como sejam a confidencialidade, integridade e disponibilidade da informação.

As medidas a tomar para a protecção dos dados que circulam nas redes de comunicações podem ser classificadas nos seguintes grupos:

- **Preventivas** - Medidas que previnam a corrupção, alteração ou disponibilização ilegítima da informação a proteger. Nestas medidas podem ser incluídas desde a restrição do acesso físico a equipamentos ou redes, até a regras restritivas no que respeita à manipulação das mesmas.
- **Detectivas** – Medidas que deverão permitir a detecção de alteração de dados, a verificação da integridade e confidencialidade dos dados que circulam na rede, bem como a identificação do modo e por quem foram efectuadas as acções ilegítimas.
- **Reactivas** – Medidas que podem ser tomadas no caso de a informação ter sido de alguma forma comprometida. Este tipo de medidas poderá permitir a recuperação de informação perdida ou corrompida.

As medidas apresentadas são de extrema importância na definição das políticas de segurança a implementar. Só a compreensão de como a informação circula nas redes de comunicações e de como esta pode ser comprometida, permitirá a tomada de decisão e a implementação das medidas de protecção descritas em conjunto e de uma forma coerente.

As medidas de protecção são, normalmente chamadas serviços de segurança que foram descritos anteriormente.

Os riscos inerentes às redes de comunicação estão directamente relacionados com as ameaças que possam ser realizadas de forma eficaz. As ameaças normalmente descritas como não-maliciosas vêm normalmente de utilizadores que não têm experiencia com as tecnologias que operam ou por “descuidos” inconscientes. Os ataques maliciosos são efectuados com vista à obtenção de lucro para o atacante (com informação obtida ou manipulação de informação) ou com objectivos destrutivos (quer em termos de indisponibilidade de serviços ou operações, quer em termos de imagem).

Os riscos mais comuns das redes de comunicação são:

- **Acesso a informação reservada ou confidencial** – Nas redes de comunicação flui muita informação, quer sejam os dados trocados entre interlocutores como informação inerente aos protocolos utilizados. Como as redes poderão ser geridas por múltiplas entidades, e estar disponíveis a qualquer "utilizador", a possibilidade de serem escutadas é real, podendo expor dessa forma informação que poderá ser valiosa ou reservada.
- **Personificação** – Num sistema distribuído os diversos equipamentos ligados a redes de comunicações identificam-se da maneira mais apropriada para serem endereçáveis e localizáveis. A personificação passa por subverter os mecanismos de identificação ou os mecanismos de autenticação subjacentes aos de identificação, para simular o envio de mensagens de um dado equipamento. O risco imediato é o de permitir que os equipamentos ligados à rede interactuem com impostores, pensando estar a interactuar com os equipamentos legítimos.
- **Intercepção de fluxo de dados** – Consiste em iludir dois extremos de uma comunicação para que ambos pensem que estão a interagir de forma segura entre si, quando na verdade estão a interagir de forma (tecnicamente) segura com um impostor que se consegue colocar no meio do fluxo de dados. Assim, a intercepção pode facultar ao atacante a possibilidade de personificar cada um dos extremos finais perante o outro extremo, algo que é designado como ataque de interposição (*man-in-the-middle attack*).
- **Modificação de fluxo de dados** – A modificação consiste em subverter um fluxo de dados entre máquinas ou redes. A subversão pode consistir na alteração de blocos de dados dos fluxos, na troca da ordem relativa de blocos, na eliminação de blocos ou ainda na injecção de blocos no fluxo, quer totalmente fabricados quer obtidos anteriormente e adicionados fora do seu local natural.
- **Reprodução de fluxo de dados** – Consiste na repetição de parte ou da totalidade de diálogos passados de forma a obter reacções dos receptores que tragam benefícios para o atacante.
- **Negação de Serviço** – Os ataques de negação de serviços (*Denial of Service- DoS*) visam corromper ou tornar inoperacional um serviço ou uma rede. Como exemplo estão a abertura de um elevado número de conexões simultâneas para um porto TCP, ou geração de uma quantidade de tráfego elevada para um determinado serviço.

3.3. Criptografia

A criptografia é a arte ou ciência que permite escrever de forma a ocultar conteúdos (do grego krypthos, oculto + *graph*, escrever). O objectivo da criptografia é permitir que um conjunto limitado de entidades, tipicamente duas, possa trocar informação que é ininteligível para terceiros. A criptografia tem fornecido ao longo dos últimos 40 anos um conjunto de técnicas de codificação com múltiplas utilizações, entre as quais as redes de comunicações [8].

A criptografia baseia-se no uso de cifras. Uma **cifra** é uma técnica concreta de criptografia, transformado **texto em claro** num texto cifrado ou **criptograma**. A operação inversa é a **decifra**, que transforma o **criptograma** no texto em claro original.

O modelo apresentado na Figura 3-1 servirá de referência às apresentações dos diversos elementos que constituem a segurança de uma rede de comunicações. As duas entidades (emissor e receptor) para poderem cooperar e transmitir informação estabelecem um canal lógico através da definição de um caminho. Torna-se necessário identificar os aspectos de segurança para a protecção de informação relativa a um atacante, nos vectores da confidencialidade, autenticidade e integridade. Todas as técnicas para proporcionar segurança têm duas componentes:

- Uma transformação de segurança da informação a enviar. Como exemplo a cifra da mensagem, tornando-a ilegível para o atacante e a adição de código baseado no conteúdo da mensagem que possa ser utilizado para verificar a identidade do emissor. Esta transformação é efectuada através de **algoritmos** que terão como parâmetros uma chave e os dados a cifrar.
- Informação secreta partilhada pelos interlocutores e que não seja do conhecimento do atacante. Como exemplo teremos as **chaves** de cifra e decifra que, em conjunção com os algoritmos de transformação de segurança (cifra e decifra), permitem a transformação do texto simples em texto cifrado, ou a operação inversa.

Uma terceira entidade da confiança de ambos os interlocutores poderá ser necessária para possibilitar uma transmissão segura, através da distribuição das chaves aos dois interlocutores da comunicação. Esta terceira entidade poderá ser necessária para garantir a autenticidade dos interlocutores.

Existem quatros tarefas principais para desenhar um serviço de segurança:

- Desenhar um algoritmo para efectuar as transformações de segurança.
- Gerar a informação secreta (chaves) a utilizar no algoritmo.
- Desenvolver métodos para a distribuição e partilha da informação secreta.
- Especificar o protocolo a ser utilizado pelas duas entidades, que façam uso do algoritmo e da chave definida.

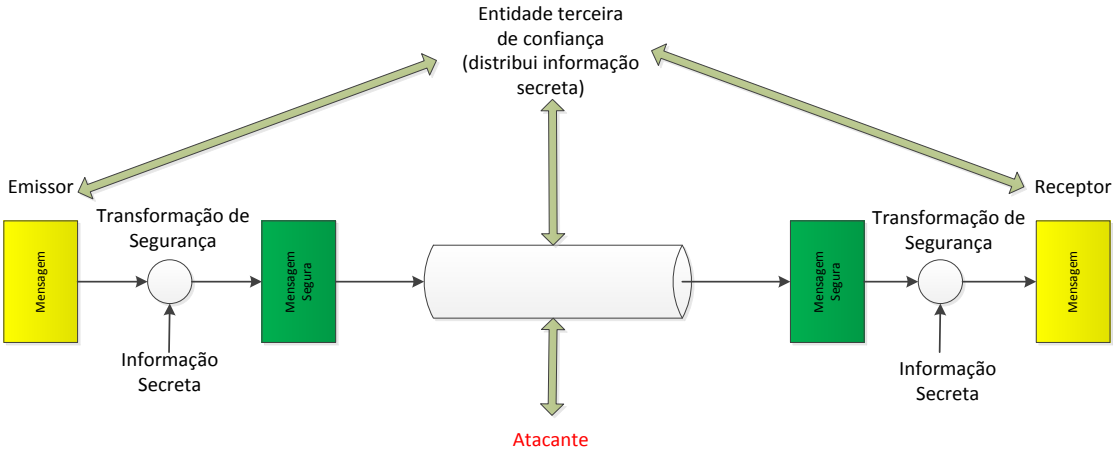

Figura 3-1: Modelo para segurança de redes

A utilização mais óbvia da criptografia é o serviço de confidencialidade. Através de um canal seguro poderá ser transmitido um texto simples desde que seja previamente cifrado, não tenho desta forma qualquer utilidade para um atacante que o capture sem que possua a chave para o decifrar.

3.4. Cifras modernas

As cifras modernas podem classificar-se segundos diversos tipos, de acordo com as suas características operacionais. Em particular podemos classificá-las segundo o seu modo de operação ou segundo o tipo de chave. Estas classificações não são exclusivas entre si.

3.4.1. Modo de operação

Segundo o modo de operação as cifras subdividem-se em **cifras por blocos** ou **cifras continuas**.

As **cifras por blocos** são cifras monoalfabéticas onde a informação, tanto em claro como criptografada, é sempre vista como uma sequência de blocos de dimensão constante de bits.

As **cifras contínuas** são cifras polialfabéticas, constituídas por um gerador pseudo-aleatório seguro cuja saída é somada ao módulo 2 (*bitwise exclusive-OR XOR*) com o texto original ou o criptograma (Figura 3-2). Assim, cada caracter do texto original, seja qual for a sua dimensão, será sempre traduzido numa cifra para outro caracter de igual dimensão, mas a tradução dependerá do estado de operação da cifra continua.

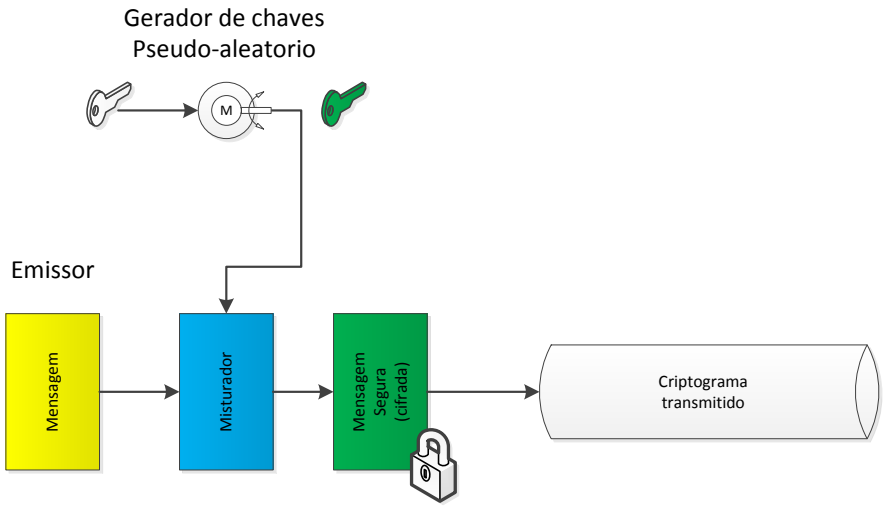

Figura 3-2: Cifra contínua

3.4.2. Tipo de chaves

Segundo o tipo de chave, as cifras subdividem-se em cifras simétricas e cifras assimétricas. Existem também a combinação das duas, muito utilizada e vulgarmente designada por cifra mista ou cifra hibrida.

3.4.3. Criptografia de chave simétrica

A cifra simétrica, também conhecida por cifra de segredo partilhado, ou cifra de **chave secreta (**Figura 3-3**)**, usa um valor comum conhecido por ambos os interlocutores - emissor e receptor - tanto para cifrar como para decifrar os dados. No contexto de troca de informação através de

uma rede, um emissor cifra os dados em claro com a chave secreta e o receptor decifra a mensagem cifrada com a mesma chave, obtendo desta forma o texto original.

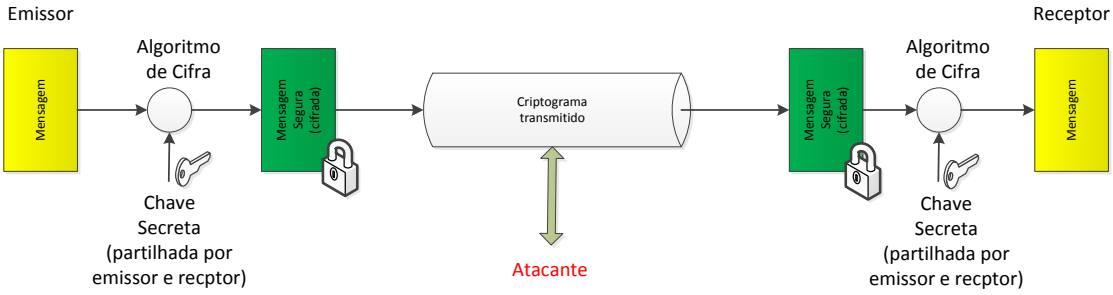

Figura 3-3: Cifra de chave secreta

Só os detentores da chave secreta podem decifrar a informação cifrada com a mesma. Assim, estas cifras destinam-se a:

- Garantir a confidencialidade dos dados apenas pela entidade que possua a chave secreta.
- Garantir a confidencialidade dos dados trocados entre duas ou mais entidades desde que partilhem a mesma chave.

As cifras simétricas têm como principal vantagem o facto de serem normalmente muito eficientes e mais rápidas relativamente às cifras assimétricas. No entanto apresentam diversas desvantagens, das quais a principal é o facto de requererem $nx(n-1)/2$ chaves para n interlocutores.

O maior desafio em termos administrativos que se coloca na utilização de chaves simétricas é a coordenação e distribuição segura das chaves secretas entre emissores e receptores. Quem quer que seja que intercepte a chave em trânsito poderá mais tarde ler, modificar ou forjar todas as mensagens cifradas ou autenticadas usando essa chave.

Cifras por blocos

Os algoritmos de cifra simétrica mais conhecidos por ordem cronológica são: DES (*Data Encryption Standard*), 3DES (*Triple DES*), IDEA (*International Data Encryption Algorithm*) e AES (*Advanced Encryption Standard*).

O DES foi inventado em 1977 pela IBM como um algoritmo de cifra público com uma chave secreta de 56 bits e um tamanho de bloco de 64 bits [8]. O DES é baseado num mecanismos de permutação e de portas OR Exclusivo. Estas operações são rápidas, tornando o DES muito

eficiente, mas ataques de força bruta permitem que seja encontrada a chave de cifra, através do teste de todas as possíveis combinações da chave. No entanto, este não é o único método de ataque possível. Em 1993 foi anunciado por *Eli Biham* e *Adi Shamir* uma técnica conhecida por criptoanálise diferencial [9] [10] e no mesmo ano foi desenvolvido outro ataque conhecido como criptoanálise linear por *Mitsuru Matsui* [11] apresentado no Eurocrypt'93 e formalizado em 1994 por *Eli Biham*.

O 3DES aplica três vezes o algoritmo DES consecutivamente, utilizando uma chave de tamanho máximo 168 bits (3*56=168), aplicada sobre o mesmo bloco com 64 bits.
O algoritmo IDEA ganhou muita visibilidade por ter sido utilizado no PGP para evitar as chaves reduzidas do DES (usa chaves de 128 bits) e é considerado por muitos como uma boa cifra, desenhada segundo princípios sólidos e bem explicados [12]. No entanto o IDEA nunca foi padronizado.

Em 1996 o NIST iniciou o processo de substituição do DES por uma outra cifra mais moderna e segura, designada por AES. Para isso solicitou em 1996 a apresentação de propostas de cifras que cumprissem determinados critérios, nomeadamente:

1. Que fossem flexíveis na definição do comprimento do bloco e da chave e que suportassem, pelo menos, blocos de 128 bits e chaves de 128, 192 e 256 bits.
2. Que fossem eficientes a executar em processadores de 32 e 64 bits
3. Que fossem facilmente implantáveis em cartões inteligentes com processadores de 8 bits.

As 15 propostas recebidas até Junho de 1998 foram discutidas e avaliadas publicamente para eleger as melhores cinco, anunciadas em Maio de 1999. Em Outubro de 2002 o NIST anunciou a escolha do algoritmo belga *Rinjdael* para AES [13].

A Tabela 3-1 compara as principais características das cifras de blocos AES e DES [14].

Tabela 3-1: Comparação entre AES e DES

Factores	DES	AES
Tamanho da chave [bits]	56	128, 192 ou 256
Tamanho do Bloco [bits]	64	128, 192 ou 256
Tipo de cifra	Simétrica por blocos	Simétrica por blocos
Desenvolvida em	1977	2000
Núm. de chaves possíveis	2^{56}	2^{128}, 2^{192}, 2^{256}
Tempo necessário para obter a chave	22 Horas	$5x10^{21}$ anos (chave de 128 bits)
Resistência à criptoanálise	Vulnerável à criptoanálise linear e diferencial; tabelas de substituição fracas	Resistente a ataques de criptoanálise diferencial, linear, interpolação.
Segurança	Considerado inadequado	Considerado seguro

Modos de cifras

Os algoritmos simétricos podem trabalhar de acordo com determinados modos. Um modo de cifra estabelece um modelo de aplicação de um algoritmo de cifra a um texto de dimensão arbitrária. Ao invés dos algoritmos de cifra, os modos de cifra não usam chaves para alterar o seu comportamento. Existem dois tipos genéricos radicalmente diferentes de modos de cifra.

Um dos tipos de modos de cifra efectua um pré-processamento dos dados antes de serem transformados pelo algoritmo de cifra no emissor e um pós-processamento do resultado no receptor após a decifra. Exemplos destes modos de cifra são o ECB e o CBC, propostos inicialmente para o DES [15].

O outro tipo de modo de cifra consiste em usar um algoritmo de cifra por blocos para realizar cifra contínua. O algoritmo de cifra por blocos é usado para calcular o estado seguinte da máquina de estados do gerador de chaves continua. Exemplo de modos de cifra deste tipo são o OFB (*Output feedback*) e o CFB (*Cipher feedback*) [15].

O modo de cifra ECB (*Electronic Code Block*) é o método mais simples e intuitivo de usar uma cifra por blocos. Consiste em dividir o texto a cifrar em blocos independentes e contínuos de igual dimensão, que são cifrados independentemente (Figura 3-4). Na decifra é seguido o mesmo processo.

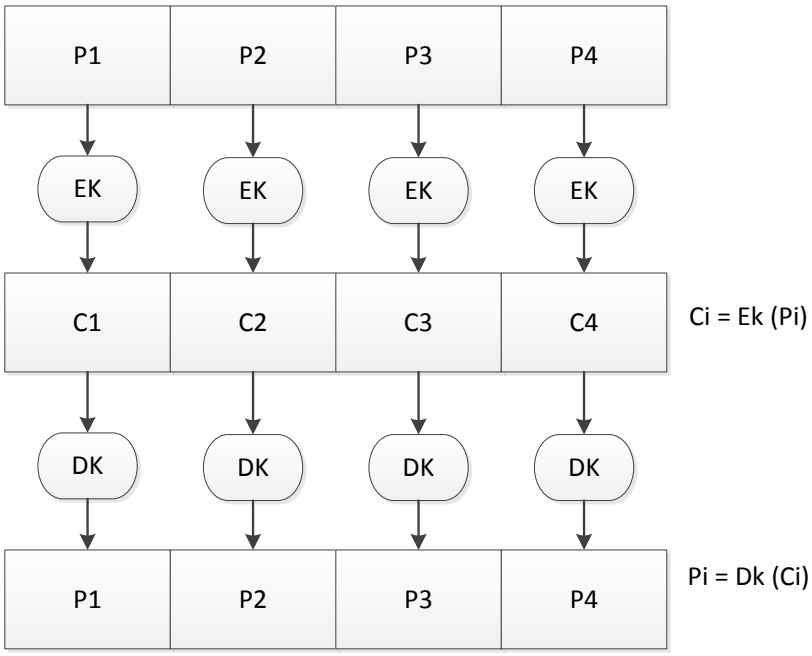

Figura 3-4: Modo de cifra ECB

Uma das fraquezas do ECB é a reprodução de padrões do texto original, porque dois blocos iguais do texto original produzem dois blocos iguais do criptograma.

Para resolver este problema existem outros modos de cifra, nomeadamente o CBC (*Cipher Block Chaining*).

O modo de cifra CBC opera de modo semelhante ao ECB, mas na cifra de cada bloco é introduzida realimentação: o texto em claro a cifrar é previamente somado ao módulo 2, com o bloco do criptograma anterior. Na decifra é seguido o processo inverso, ou seja cada bloco decifrado é somado com o bloco anterior do criptograma para recuperar o bloco de texto original (Figura 3-5).

O vector de inicialização (VI) usado para processar o primeiro bloco pode ser secreto ou não. A segurança introduzida pelo CBC não depende do secretismos do VI, uma vez que se destina fundamentalmente a evitar repetição de padrões do ECB.

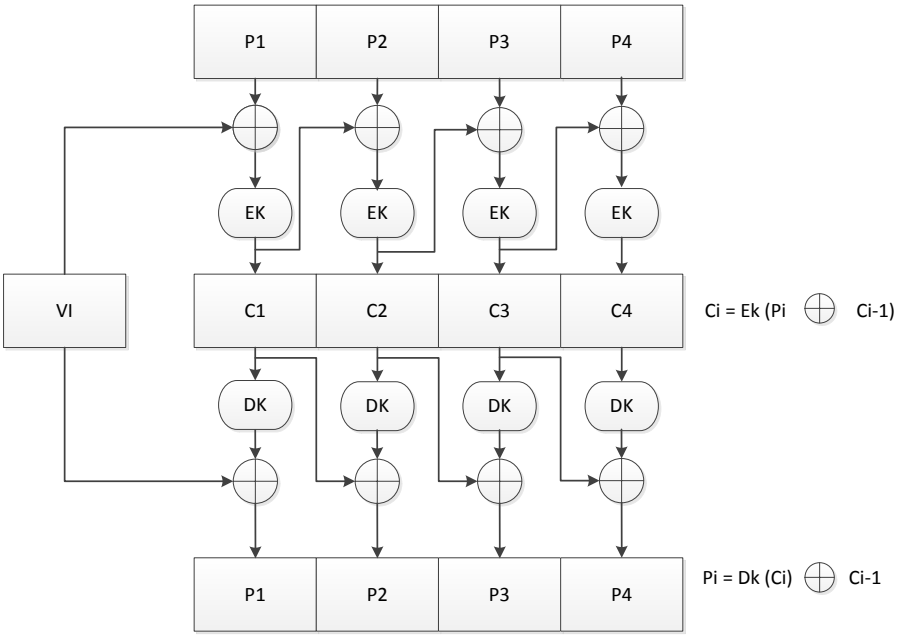

Figura 3-5: Modo de cifra CBC

Cifra continua

Uma cifra continua, tal como já referido anteriormente utiliza um gerador pseudo-aleatório de chaves que opera em função de uma chave de tamanho fixo e reduzido (ex: 128 bits), que produz uma chave continua (*keystream*) que é operada juntamente com o texto original ou o criptograma, consoante se esteja a cifrar ou decifrar (Figura 3-2).

A grande maioria dos algoritmos de cifra contínua são síncronos, ou seja, a operação XOR bit a bit, do gerador é independente dos dados cifrados e decifrados, o que obriga os dois extremos da comunicação a gerirem o sincronismo.

Aspectos importantes no desenho de cifras contínuas [8]:

- A sequência cifrada deverá ter um período longo. O gerador pseudo-aleatório utiliza uma função que produz uma sequência contínua de bits que eventualmente se repetirá. Quanto maior o período de repetição, maior a dificuldade na criptoanálise.
- A chave contínua deve possuir propriedades de verdadeiro número aleatório contínuo. Por exemplo, o número de 1 e 0 deve ser aproximadamente igual. Se for tratada como uma sequência de bytes todas os valores das 256 possibilidades devem aparecer com frequências semelhantes.

- A saída do gerador pseudo-aleatório é condicionada por uma chave de tamanho fixo e pequeno. Para prevenir um ataque de força bruta, esta deverá ter o maior tamanho possível.

Os algoritmos de cifra simétrica contínua mais usados, na prática ou em normas, são o A5 e o RC4. O A5 é o algoritmo de cifra usado em comunicações GSM (*Global System for Mobile communications*).

O RC4 é um algoritmo desenvolvido pela RSA em 1987, por *Ron Rivest*, sendo uma das cifras contínuas mais utilizadas, como sejam nos protocolos de comunicação SSL/TLS (*Secure Sockets Layer/Transport Layer Security*) e no WEP (*Wired Equivalent Privacy)*, em redes sem fios. Uma das vantagens do RC4 é a sua simplicidade e rapidez, mas tem vulnerabilidades caso seja utilizado de forma incorrecta [16].

A cifra contínua RC4 é composta por dois componentes, representados na Figura 3-2: um algoritmo de mistura de chaves, KSA (*Key Scheduling Algorithm*), e um algoritmo que gera a chave contínua, designado por PRGA (*Pseudo Random Generator Algorithm*)

KSA(K, keylen)	*PRGA (len)*
# Preencher o vector S-Box com valores de 0 a 255 *for i=0 to 255 do* *S[i] = i;* *T[i] = K [i mod keylen]* *end for* *# Permutação de S-Box usando a chave K* *j=0* *for i=0 to 255 do* *j = (j + S[i] + T[i]) mod 256* *swap(S[i], S[j]);* *end for*	*i=0, j=0* *#ciclo de geração de Z* *For k=0 to len – 1* *i = (i+1) mod 256* *j = (j+S[i]) mod 256* *Swap(S[i], S[j])* *t = (S[i] + S[j]) mod 256* *z = S[t]* *end for* *#retorna byte da chave continua "z"*

O RC4 utiliza o conceito de estados nos processos de cifra e decifra. Uma chave variável de 1 a 256 bytes (8 até 2048 bits) é utilizada para inicializar um vector de estados de 256 bytes designado por S-box (S[0] até S[255]). A chave de cifra é representada por K e tem comprimento *keylen*.

O algoritmo de mistura de chaves, KSA, é executado em função do valor e do comprimento da chave K. Na fase inicial o vector S é preenchido com valores de 0 a 255 (S[0]=0, …, S[255]=255). É criado um vector temporário T, para o qual são transferidos os primeiros *keylen* elementos da chave K e repetido o processo até ao preenchimento de todos os 256 bytes de T. De seguida é utilizado o vector T para produzir a permutação inicial de S. Esta operação envolve começar no S[0] e ir até S[255], e por cada S[i], trocar o S[i] por um outro elemento do vector S, de acordo com o esquema indicado por T[i].

Após o cálculo do vector de estados S, o RC4 passa ao processo de cifra. Para isso necessita de obter cada byte Z da chave continua através do algoritmo gerador, PRGA.

Para cifrar o texto em claro apenas é necessário efectuar um XOR entre o valor da chave continua "Z" e o próximo byte do texto em claro.

Vector de inicialização utilizado no RC4

A utilização de um vector de inicialização, IV (*Initialization Vector*), pretende solucionar um problema inerente à utilização de algoritmos de chave simétrica contínua com tamanho de chave secreta fixo. Neste tipo de algoritmo se a chave de cifra contínua for utilizada mais do que uma vez para cifrar o mesmo texto plano, resulta que o texto cifrado será o mesmo. Este resultado permite a um atacante determinar matematicamente o valor da chave contínua. A solução para este problema passa pela utilização de um vector de inicialização. Em vez de se utilizar uma chave secreta de tamanho fixo, esta pode ser combinada com um vector de inicialização, que é alterado em cada pacote, criando desta forma uma chave diferente para cada pacote cifrado. Em teoria, o conhecimento do IV não tem qualquer utilidade sem o conhecimento da chave secreta, desde que o mesmo IV não seja utilizado duas vezes com a mesma chave secreta.

3.4.4. Criptografia de Chave Pública ou cifras assimétricas

O conceito de criptografia de chave pública apareceu em resposta a dois problemas associados à cifra simétrica.

O primeiro problema estava associado ao processo de distribuição da chave secreta. Tal como já referido, a distribuição de chaves secretas da cifra simétrica requer que os dois interlocutores partilhem da mesma chave, que de alguma forma lhes foi entregue, ou a utilização de um

sistema de distribuição de chaves. *Whitfield Diffie* e *Martin Hellman* [17] afirmaram que este prossuposto negava a essência da criptografia, pelo facto de haver uma terceira entidade com conhecimento de uma chave secreta, e apresentaram em resposta a criptografia de chave pública.

O segundo problema que Diffie apresentou, que não está relacionado com o anterior, consiste no conceito de assinatura digital. A necessidade de troca de informação, que em analogia com o mundo físico, permitissem assinar documentos ou mensagens, teria grande aplicabilidade militar ou comercial.

Em 1976 *Diffie* e *Hellman* apresentaram um método que procurava resolver ambos os problemas e que se traduzia na criptografia de chave pública.

As cifras assimétricas ou de chave pública baseiam-se na utilização de duas chaves de cifra distintas mas relacionadas - uma pública e outra privada - não sendo possível cada uma das chaves calcular a outra chave correspondente. Ambas as chaves são geradas ao mesmo tempo e têm funções complementares visto que a cifra efectuada com uma delas necessita da outra para o processo de decifra. Cada uma das duas chaves é utilizada numa função específica. A chave privada deverá ser do conhecimento de apenas uma entidade e poderá ser utilizada para além da cifra para autenticação ou autoria. A chave pública pode (e deve) ser publicitada, possibilitando que outras entidades validem a autoria ou autenticação de determinada informação cifrada que recebem. As chaves utilizadas neste tipo de cifra estão relacionadas matematicamente, conseguindo uma decifrar o que a outra cifrou. Uma das propriedades principais deste tipo de sistema é que dada uma chave é computacionalmente impossível determinar a outra.

Em termos operacionais as cifras assimétricas têm como principal vantagem o facto de exigirem menos chaves para efectuar iterações seguras, porque permitem uma relação de muitos para 1. Num universo de N interlocutores, para efectuar qualquer troca de dados confidencial entre qualquer par deles, só é preciso usar Nx2 chaves diferentes (privada + pública). Ou seja, o número de chaves cresce linearmente com a população. A principal desvantagem é o facto de serem muito pouco eficientes porque se baseiam em operações matemáticas complexas. Por exemplo o RSA [18] desenvolvido por *Ronald Rivest, Adi Shamir* e *Leonard Adleman* em 1997 é aproximadamente 1500 vezes mais lento que o DES.

Em termos administrativos os principais problemas subjacentes à utilização de criptografia assimétrica são:

- Confinamento rigoroso das chaves privadas aos seus legítimos detentores
- A distribuição fidedigna das chaves públicas a todos os que as pretendam usar
- Gestão do tempo de vida dos pares de chaves

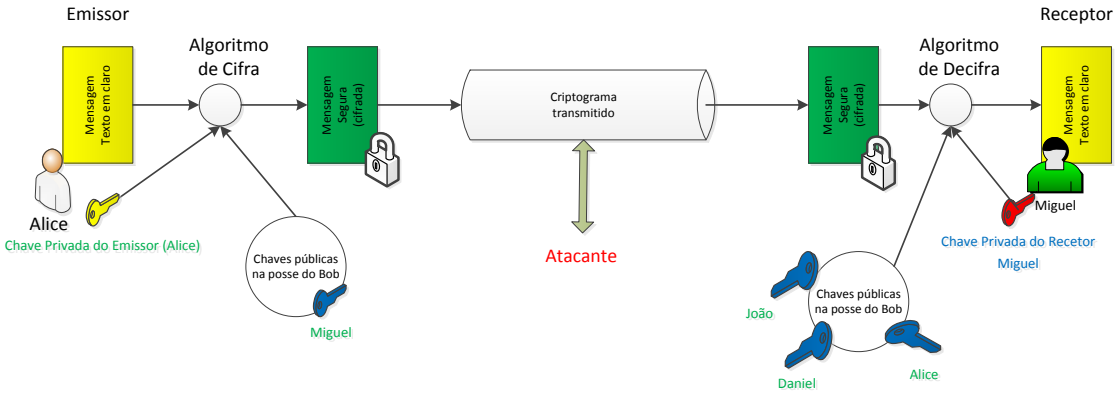

Figura 3-6: Criptografia de chave pública

Tomando como exemplo a Figura 3-6, cada utilizador (Alice e Miguel) possui um par de chaves distintas, uma chave privada e uma chave pública. A chave pública é disponibilizada aos utilizadores com que se pretende comunicar. Assim é possível ao emissor (Alice) enviar uma mensagem cifrada com a chave pública do receptor (Miguel), com a garantia de que a mensagem é apenas decifrada por este, utilizando a sua chave privada, garantindo desta forma a **confidencialidade** da informação.

Por outro lado, se o emissor (Alice) cifrar uma mensagem com a sua chave privada, esta poderá ser lida por todos os receptores que possuírem a sua chave pública, assegurando assim a origem da mensagem, ou seja a **autoria**. Este é o mecanismo básico para a implementação de assinaturas digitais.

3.4.5. Criptografia híbrida

As cifras mistas ou **híbridas** (Figura 3-7) surgiram como uma solução intermédia muito utilizada na troca confidencial de mensagens, tentando juntar o que há de melhor nas cifras simétricas e assimétricas. Na prática, a cifra de dados é feita utilizando um algoritmos de cifra simétrico (3DES por exemplo), e é utilizado um algoritmo de chave pública (RSA), com a

chave pública do receptor, para cifrar a chave simétrica (secreta) que é enviada ao receptor em conjunto com os dados cifrados. Deste modo consegue-se uma eficiência muito próxima da obtida nas cifras simétricas, sem a desvantagem de ter de transmitir a chave secreta por um canal seguro externo.

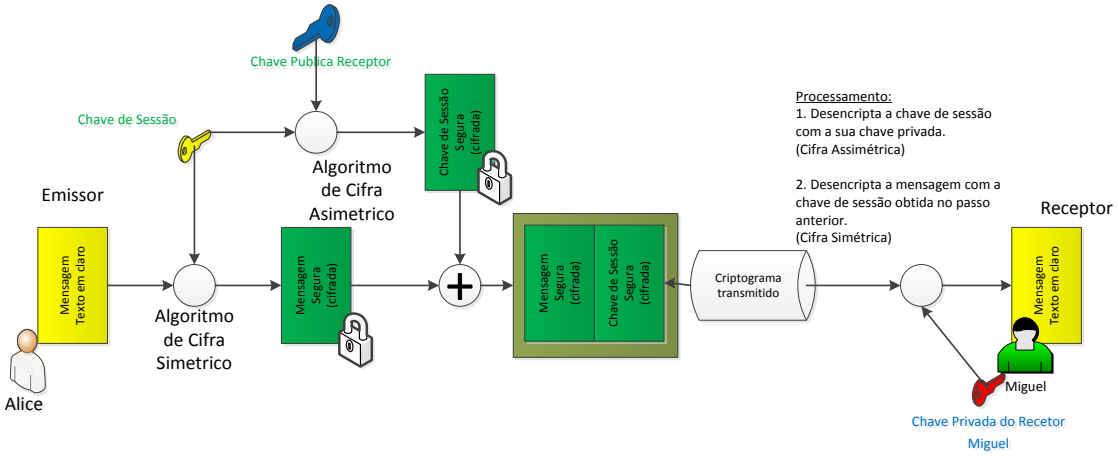

Figura 3-7: Cifra híbrida

Para decifrar a mensagem o receptor deverá utilizar a sua chave privada em primeiro lugar para decifrar a chave de sessão. Com esta, o receptor decifra a mensagem e tem acesso ao seu conteúdo.

3.5. Funções de síntese (*Hash*)

As funções de síntese, ou funções de *hash* não são propriamente funções criptográficas, uma vez que não servem para cifra ou decifrar dados, mas são úteis para complementar, com segurança criptográfica, outros mecanismos de segurança. Uma função de síntese converte um bloco de dados de tamanho variável, num resultado de tamanho fixo, normalmente muito mais pequeno que o bloco de dados original. Para o conseguir aplicam, interactivamente, uma função de compressão, que trata e produz dados de dimensão constante.

Este tipo de funções é muito utilizado em processos de criptografia assimétrica. Como principais propriedades destacam-se:

- O resultado é um bloco de tamanho limitado e constante (16 ou 20 bytes);
- É computacionalmente impraticável encontrar dois blocos de dados diferentes cujo resultado de *hashing* seja igual (sem colisões);
- Impossibilidade de recuperar uma mensagem original a partir do valor de *hash*;

Existem diversos termos para designar as funções de síntese como sejam funções irreversíveis, funções de um único sentido, funções *digest*, ou funções *fingerprint*.

Actualmente existem diversas implementações como sejam a série de funções MD (*Message Digest*) MD2, MD4 e MD5 desenvolvidas pela RSA que devolve um valor (*fingerprint*) de 128 bits (16 bytes) ou outros algoritmos como o SHA-1, SHA-256 ou SHA-512 [19] [20], projectados pela NSA que devolvem valores de 160, 256 e 512 bits respectivamente.

Actualmente o MD5 [21] e o SHA-1 [20] são os mais usados, apesar de já terem sido descobertas vulnerabilidades em ambos [22]. Um grupo de investigadores descobriu um método expedito de cálculo de colisões, provando que o MD5 é um algoritmo bastante vulnerável [23].

3.6. Autenticadores de dados

Os autenticadores de dados são conjuntos de bits que acompanham a mensagem e que permitem:

- Permitir ao receptor autenticar a origem da mensagem
- Provar a integridade da mensagem

Os valores gerados a partir das mensagens, a partir das funções síntese não são por si só suficientes para este fim, porque apenas garantem a prova da integridade da mensagem. Para assegurar a origem os autenticadores têm que incluir na sua geração e validação dados secretos (chaves) ou cifras. Consoante a utilização de criptografia simétrica ou assimétrica, teremos autenticadores de mensagens (*Message Authentication Code*, *MAC*) ou assinaturas digitais.

3.6.1. Autenticadores de mensagem (MAC)

Um autenticador de mensagem (*Message Authentication Code*, *MAC*) é um valor produzido a partir de uma mensagem e de uma chave secreta simétrica, partilhada entre o emissor e o receptor.

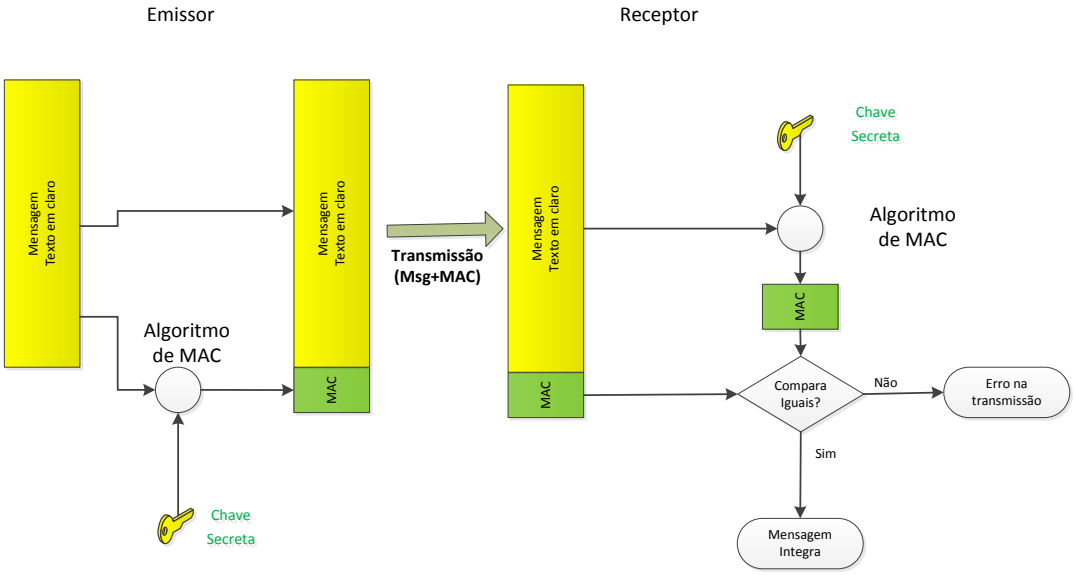

Figura 3-8: Geração e verificação do MAC

O processo mais simples de utilização de MAC, descrito na Figura 3-8, consiste nos seguintes passos:

- O emissor aplica uma função de síntese sobre a mensagem, usando uma chave secreta, produzindo um MAC;
- O emissor envia a mensagem juntamente com o MAC para o receptor;
- O receptor ao receber uma mensagem aplica a mesma função de síntese, com a mesma chave secreta, sobre a mensagem produzindo um $MAC_{rec.}$
- O receptor compara o MAC recebido juntamente com a mensagem e compara-o com o MAC_{rec} calculado. Se os valores forem iguais, fica provado que a mensagem está íntegra e não foi adulterada.

Há várias maneiras de enquadrar o autenticador MAC adicionando a vertente de confidencialidade através da cifra das mensagens:

- Produzir um MAC a partir de uma mensagem em claro e enviá-lo em claro junto com a mensagem cifrada. O SSH usa esta combinação na produção de mensagens seguras;
- Produzir um MAC a partir da mensagem em claro e cifrá-lo em conjunto com a mensagem (Figura 3-9). O SSL usa esta combinação na produção de mensagens seguras;
- Cifrar a mensagem e produzir um MAC a partir do criptograma resultante. O IPSec usa esta combinação na produção de *datagramas* seguros.

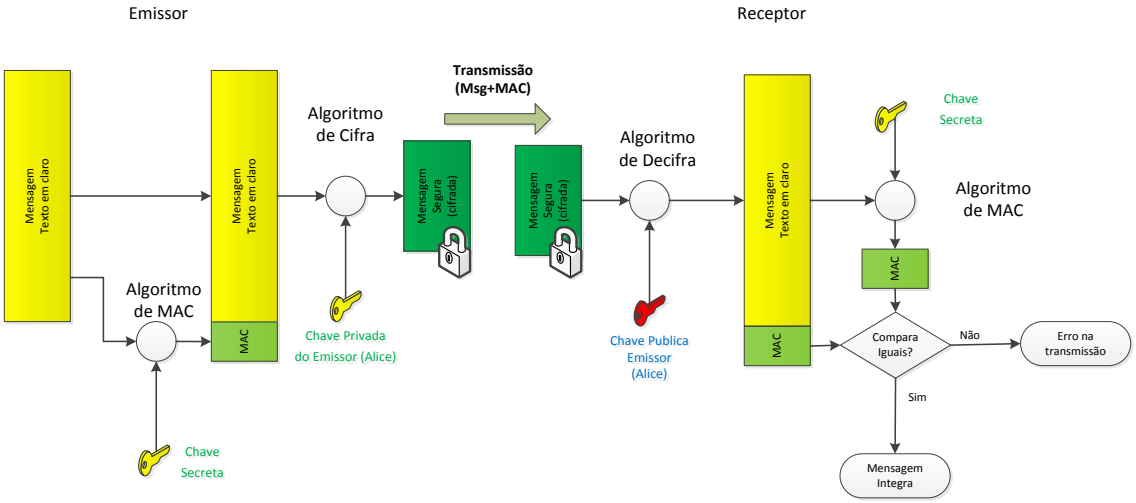

Figura 3-9: Autenticação e confidencialidade com MAC

3.6.2. Assinatura digital

As assinaturas digitais são um mecanismo de prova da origem dos dados, garantindo a autoria perante terceiros e um mecanismos de integridade dos dados transmitidos (sendo apenas válida para os dados originais). A assinatura digital permite garantir o não repúdio e a associação apenas a uma e só uma entidade emissora, podendo ser validada universalmente (não repúdio). As assinaturas digitais são sempre únicas conforme o documento que autenticam. Naturalmente a criptografia assimétrica é a que melhor se adequa a este fim.

Um método de assinatura digital, recorrendo a criptografia assimétrica, consiste na cifra de um documento com a chave privada do emissor (ou autor), enviando depois o criptograma para o receptor juntamente com a mensagem em claro. Neste caso o receptor utiliza a chave pública do emissor para verificar a validade da assinatura digital, através da aplicação do algoritmo de decifra sobre a mensagem em claro e compara-a com o criptograma recebido. Caso sejam iguais garante-se a autoria e integridade do documento. Este processo pressupõe que o criptograma terá o mesmo tamanho aproximado do documento, fazendo duplicar o volume de dados a transmitir.

Para optimizar este esquema introduziu-se uma função de síntese no processo de assinatura digital (Figura 3-10). Mais especificamente, a assinatura digital é o resultado da cifra da síntese da mensagem, efectuada com a chave privada do emissor. Qualquer alteração na mensagem

produz uma síntese diferente e consequentemente um criptograma diferente. Após este cálculo é enviada a mensagem em claro junto com o criptograma produzido.

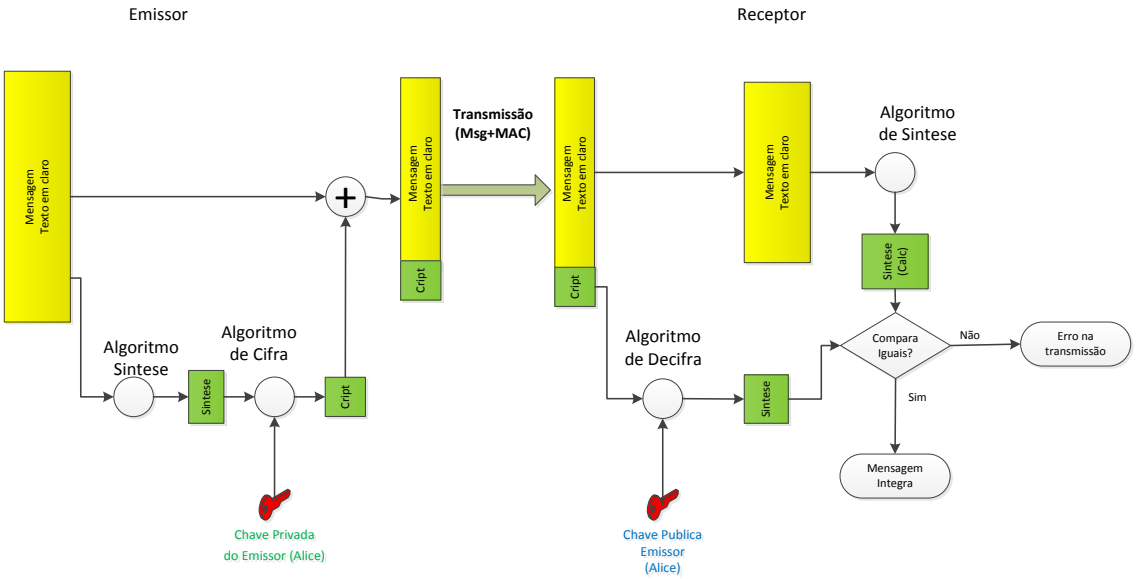

Figura 3-10: Assinatura digital RSA

Quando o receptor recebe a mensagem calcula um valor de síntese (*SinteseCalc*) sobre o texto em claro recebido, decifra com a chave pública do emissor o criptograma recebido e obtém o valor de síntese (*Sintese*) recebido. Se o valor de síntese calculado (*SinteseCalc*) e o recebido (*Sintese*) forem iguais significa que o conteúdo da mensagem não foi alterado e que a integridade da transmissão e a autenticação do emissor está garantida.

A assinatura digital fornece *per si* apenas autenticidade e integridade, mas não confidencialidade. Para garantir a confidencialidade dos dados, estes terão que ser cifrados, obtendo-se assim um serviço designado por envelope digital assinado (Figura 3-11).

Os algoritmos de assinatura mais usados, na prática ou em normas, são o RSA e o DAS (*Digital Signature Algorithm*)

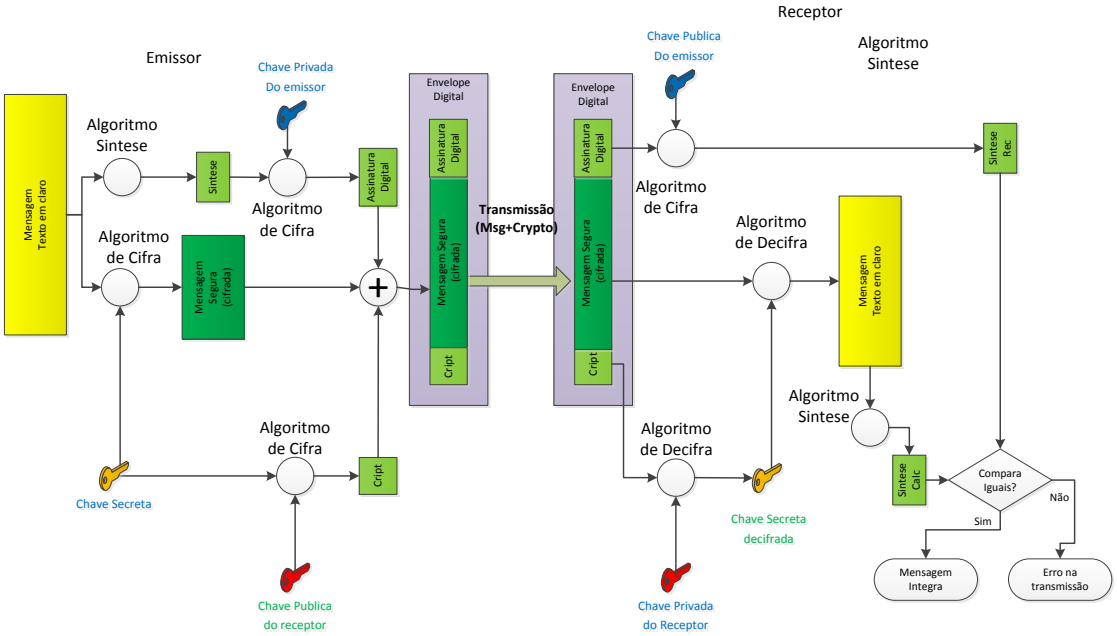

Figura 3-11: Envelope digital

3.7. Gestão e distribuição de chaves

A utilização de chaves simétricas ou assimétricas é fundamental para a garantia da confidencialidade e integridade da comunicação entre entidades, para além de poderem fornecer também a função de autoria. Um grande número de mecanismos de segurança depende da utilização desta chaves, pelo que é de extrema importância garantir que a geração, distribuição e manutenção das mesmas seja feita de um modo seguro.

O processo de geração de chaves inclui entre outras, as seguintes tarefas:

- Na produção das cifras devem-se assegurar um conjunto de propriedades, como por exemplo a aleatoriedade;
- A divulgação ou distribuição das chaves deve ser efectuada de forma a garantir a privacidade e integridade das chaves e que apenas serão entregues às entidades que delas necessitem;
- Cada entidade deverá proteger as chaves que lhe foram fornecidas, por forma a que não sejam adulteradas ou capturadas por terceiros de forma ilegítima;
- No caso das chaves públicas deverá também ser garantida uma correcta distribuição;

O método utilizado para a gestão e distribuição é diferente dependendo do tipo de chaves (simétricas ou assimétricas) que se pretende gerir.

3.7.1. Distribuição de chaves simétricas

Nos sistemas simétricos é necessário fazer chegar a duas entidades uma chave secreta, por forma a proteger a comunicação entre si. Esta chave deverá ser distribuída de forma a manter-se secreta para os restantes participantes no sistema de comunicações. Existem vários métodos de distribuição de chaves simétricas entre os quais se destacam o *Diffie-Hellman* e o RSA.

3.7.1.1. Algoritmo de *Diffie-Hellman*

O algoritmo de *Diffie-Hellman* é um algoritmo de distribuição de chaves de sessão (simétricas) que foi apresentado em 1976 [24]. Este algoritmo usa conceitos da teoria dos números e baseia a sua segurança na dificuldade de cálculo de logaritmos modulares de grandes números. Esta técnica permite a duas entidades a criação e troca de uma chave secreta que poderá ser utilizada como chave de sessão num sistema de cifra simétrica.

O algoritmo usa valores públicos globais e valores públicos apresentados por cada uma das partes para calcular um valor secreto ao qual só os interlocutores podem chegar em conjunto.
O protocolo tem dois parâmetros de sistema *p* e *g*. O parâmetro *p* é um número primo maior que 2 e o parâmetro *g* é uma raiz primitiva "*mod p*", ambos públicos e conhecidos pelos interlocutores.

O parâmetro *q* possui a seguinte propriedade:

- Para cada número *n* entre 1 e *p-1* inclusive, existe uma potência *k* de *g* tal que:

$n = g^k \bmod p$

1. Ambos os interlocutores A e B geram valores secretos (preferencialmente aleatórios) *a* e *b* e calculam:

   A calcula: $n_A = g^a \bmod p$

   B calcula: $n_B = g^b \bmod p$

2. Feito este cálculo A envia para B o valor de n_A e B envia para A o valor de n_B. Estes valores são designados por **valores públicos de Diffie-Hellman**.
3. Após troca dos valores públicos cada um dos interlocutores consegue calcular de forma independente um valor comum secreto K:

   A calcula: $K = (n_B)^a \bmod p = g^{ba} \bmod p$

   B calcula: $K = (n_A)^b \bmod p = g^{ab} \bmod p$

Se o valor de *p* for muito grande (na ordem de centenas ou milhares de bits) e se *(p-1)/2* for igualmente um valor primo, então nenhum atacante que conheça *p*, *g*, n_A e n_B consegue calcular K [25]. Se para além disso, os valores secretos de *a* e *b* forem gerados aleatoriamente, se forem convenientemente protegidos durante a execução do algoritmo e se forem descartados logo após o cálculo de K então o valor de K (chave) possui a segurança futura perfeita (*Perfect Forward Secrecy* - PFS).

3.7.1.2. Distribuição de chaves simétricas com RSA

Os sistemas de chaves públicas também podem ser utilizados para implementar sistemas de distribuição de chaves simétricas de sessão. Assim, é suficiente que cada entidade estabeleça o seu par de chaves privada / pública (Figura 3-12) para pode trocar chaves simétricas com outras entidades intervenientes na comunicação que tenham também pares de chaces privada/pública.

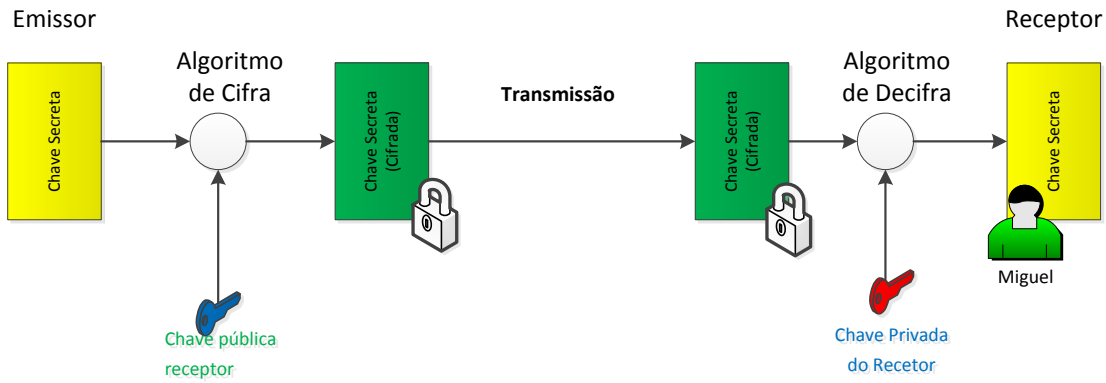

Figura 3-12: Distribuição de chaves simétricas com RSA

3.7.2. Distribuição de chaves públicas

A criptografia assimétrica é uma das formas actuais de trabalhar com cifras que permite que muitas entidades enviem dados secretos para uma só entidade, usando apenas uma chave pública, e que muitos validem a assinatura digital associada a um documento usando apenas a chave pública do assinante. Em ambos os casos é fundamental que a chave pública seja a correcta, ou seja, que corresponda à entidade verídica.

O principal problema associado aos mecanismos de chave assimétrica é a distribuição das chaves públicas. A distribuição deve assegurar a autenticidade e integridade das chaves públicas entre as entidades intervenientes. Não deve ser possível que uma entidade ilegítima altere ou

substitua uma chave pública de uma entidade. Se tal acontecesse, poria em causa a confidencialidade de dados cifrados por um emissor (através da chave pública alterada) que fossem enviados para a entidade receptora, visto que uma entidade atacante poderia ter acesso aos mesmos.

Apresentam-se agora algumas das técnicas para a distribuição de chaves assimétricas.

Distribuição manual

A distribuição manual de chaves públicas consiste na troca das chaves públicas entre duas entidades de forma directa e explícita. Esta troca pode ser feita presencialmente ou sob a forma electrónica, havendo neste caso um conjunto de canais de comunicação alternativos por forma a que se confirme a correcção dos dados recebidos. Os canais alternativos destinam-se a evitar que um atacante consiga subverter todo um processo de distribuição manual controlando apenas um canal de comunicação.

Distribuição embebida

Este método é uma das formas mais comuns actualmente de distribuição de chaves públicas através de produtos de *software*, como sejam os navegadores. Estes são uma das ferramentas que mais usam a criptografia assimétrica, sobretudo para autenticar serviços ou servidores remotos. Esta forma de distribuição, apesar de apresentar alguns riscos de manipulação ou alteração de chaves públicas, é universalmente usada para a importação das chaves públicas das raízes de cadeias de certificação (Figura 3-13).

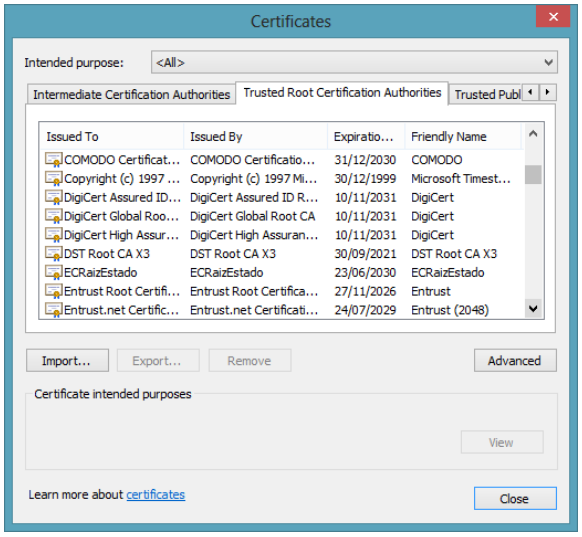

Figura 3-13: Distribuição embebida de chaves públicas

Distribuição interactiva

Existem diversos protocolos em que as chaves públicas, usadas para autenticar interlocutores, são distribuídas no âmbito da execução desses protocolos (ex: SSL/TLS [26], SSH, IPSec [27]), podendo nestes casos distribuir-se chaves públicas ou certificados das mesmas.

Distribuição *ad-hoc*

A distribuição *ad-hoc* consiste na possibilidade de importação de uma chave pública, em caso de falta da mesma, a partir de repositórios públicos. É importante que se garanta que a cópia importada é correcta, ou seja, que é mesmo a chave pública original da entidade pretendida.
Os mecanismos de distribuição *ad-hoc* de chaves públicas certificadas podem ser diversos. Podem obter-se as chaves através de servidores Web acessíveis via *http*, serviços de directoria *X.500* ou serviços de *MS Active Directory* via LDAP, entre outras.

Anúncio público

A entidade anuncia a sua chave pública através de diversos meios, incluindo-a em cada mensagem de correio electrónico ou disponibilizando-a numa página web pessoal. Esta abordagem não é considerada segura, pois um utilizador mal-intencionado pode falsificar a identidade de outro.

Directório público

A existência de um local onde residem as chaves públicas, da confiança das diversas entidades de um sistema, permite às diversas entidades, quando o necessitem, obter as chaves públicas de outros interlocutores. A segurança deste directório central é fundamental para todo o sistema, bem como a gestão do ciclo de vida das chaves.

3.8. Certificação digital e PKI (*Public Key Infrastructure*)

Na internet, diversas normas como sejam S/MIME [28], SSL/TLS, IPSec e SSH baseiam-se na utilização de chaves públicas para troca segura de mensagens. Estes têm em comum um problema fundamental: como confiar numa associação que liga uma chave pública com o seu dono. Esta ligação é particularmente crítica na autenticação de entidades (utilizadores, servidores web, etc.) e na garantia da confidencialidade e integridade das mensagens trocadas. Torna-se desta forma essencial a gestão das chaves privadas através de uma infra-estrutura de chaves públicas (PKI).

3.8.1. Infra-estrutura de chaves públicas (PKI)

Ao conjunto de entidades certificadoras (*Certification Authority*, CA) existentes num dado contexto, à sua interligação em cadeias de certificação e ao conjunto de políticas e de mecanismos de *software* e *hardware* usados para gerir os certificados, dá-se a designação de PKI (Public KeyInfrastructure).

Uma PKI suporta aspectos técnicos mas também aspectos organizacionais para desempenhar as seguintes funções:

- Definir políticas de criação de pares de chaves assimétricas de pessoas ou serviços;
- Definir políticas de emissão de certificados de chaves públicas;
- Definir políticas de revogação de chaves públicas;
- Definir cadeias de certificação;
- Gerar chaves assimétricas (púbicas/privadas) de acordo com a política;
- Distribuir as chaves aos seus donos, através da emissão de certificados de chaves públicas de entidades após prova adequada da associação entre as chaves e as entidades;
- Publicar, Validar e revogar certificados de chaves públicas.

As CA são o coração das PKI e onde se realizam as componentes operacionais. As PKI existentes actualmente na Internet tomaram a forma de entidades certificadoras organizadas de forma hierárquica em **cadeias de certificação** (Figura 3-14).

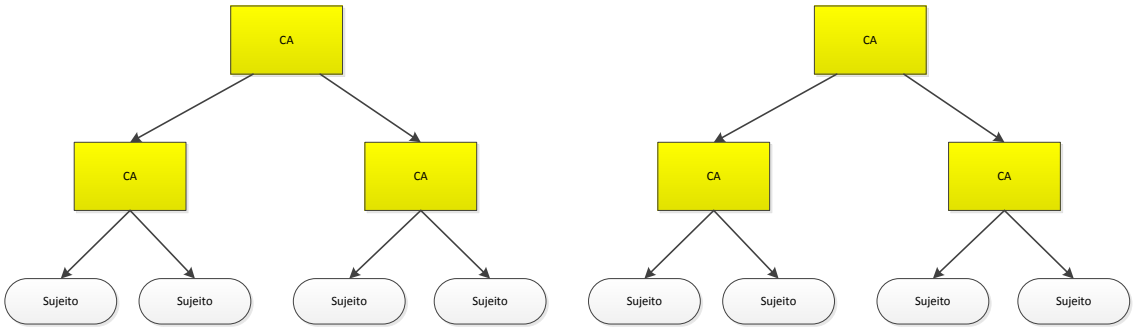

Figura 3-14: Cadeia de certificação: modelo com oligarquia

As CA no topo da hierarquia delegam autoridade de gestão de parte dos certificados em CAs inferiores (hierarquicamente). As CAs podem assumir dois tipos de papéis de autoridade:

- Entidade certificadora (CA) – A CA é a única entidade que guarda a chave privada da CA e está empossada para a emissão de certificados digitais e de listas de revogação de certificados;
- Entidades de registo (*Registration Authority-RA*) – uma ou mais entidades de registo podem estar associadas a uma CA e funcionam como um *interface* com os utilizadores. Filtram os pedidos de certificados recebidos através de controlo da identidade do requisitante. Têm também como função a publicação e validação de certificados gerados pela CA, a validação da autenticidade dos pedidos de revogação de certificados e a publicação da lista de certificados revogados.

Os serviços de PKI públicos reconhecidos de confiança, são fornecidos por CSP (*Certification Service Providers*) como sejam a *Verisign* [29], *DigiCert* [30] ou a *GeoTrust* [31].

3.8.2. Certificação digital

A certificação digital consiste na emissão de certificados digitais de chaves públicas. Os certificados são documentos com uma estrutura pré-definida que possuem entre outros elementos uma chave pública de uma dada entidade e uma assinatura digital do certificado feito pela entidade emissora do mesmo - uma entidade certificadora (CA). A assinatura digital garante a integridade da chave pública e também a sua autenticidade.

Os certificados são documentos com tempo de vida limitado, podendo ser controlados de duas formas: através de um prazo de validade não alterável dentro do certificado ou através de certificados de revogação, emitidos pela CA.

Estrutura dos certificados digitais

Existem vários tipos de certificados digitais, mas por norma obedecem à estrutura definida na recomendação X.509 do ITU-T. Esta especificação faz parte da série de recomendações X.500 que definem um serviço de directório, tendo sido publicada inicialmente em 1988. Até à data foram definidas três versões de certificados digitais (Figura 3-15).

A versão de X.509 que surgiu em 1988, e à qual foi atribuída a versão 1, não era suficientemente flexível dada a impossibilidade de adicionar novos atributos ao certificados. Em 1993, quando o padrão X.509 foi revisto, foram acrescentados dois campos aos certificados para suportar controlo de acesso, donde resultou o formato X.509 versão 2. Esta versão mantinha as limitações na incorporação de novos atributos pelo que foi revista em 1996 e definida a versão X.509 v3 [32] [33]. Esta versão suporta o conceito de extensão, onde qualquer um pode definir uma nova extensão e incluí-la nos certificados (Figura 3-16).

A norma X.509v3 define um formato base que contém um conjunto de valores obrigatórios em todos os certificados (RFC 3280 [32]):

- Versão do certificado – Versão do certificado (V1, V2 ou V3);
- Número de série – Identificador único do certificado emitido por uma CA;
- Algoritmo de Assinatura – Algoritmos usados para assinar o certificado. Normalmente são usados dois, um de síntese e outro de cifra com uma chave privada;
- Nome Emissor (*Issuer Name*) – entidade emissora do certificado;
- Período de validade – data e hora de início e fim da validade;
- Identificação do titular (*Subject name*) - Nome da entidade a quem a chave pública pertence;
- Chave pública – Chave pública do titular do certificado;
- Identificador único da CA - Fornece um valor que identifica inequivocamente a CA que gerou e emitiu o certificado no caso do nome da CA ser partilhado por diferentes entidades;
- Identificador único da entidade – Valor que identifica inequivocamente a entidade a quem o certificado pertence, caso o nome da entidade seja partilhado por diferentes entidades;
- Extensões – A norma RFC 5280 define um conjunto de extensões que indicam formas de utilização do certificado. Algumas extensões vulgarmente utilizadas são a *Key Usage*, que limita o uso das chaves a determinadas funcionalidades, como por exemplo apenas assinaturas (*Signing Only)*, e a extensão *Subject Alternative Name*, que permite que outras identificações como o nome de DNS ou o endereço de correio electrónico possam ser associadas à chave pública do certificado.
- Assinatura – Contém também a síntese relativa a todo o certificado, cifrada com a chave privada de quem (CA) gerou o certificado. Inclui também a indicação do algoritmo utilizado na criação da assinatura.

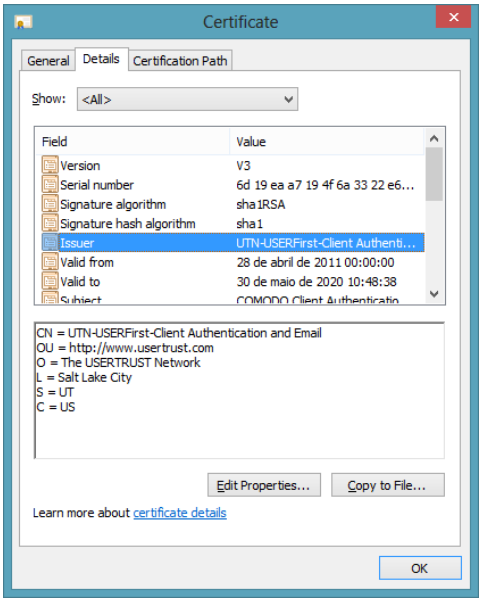

Figura 3-15: Exemplo de um certificado

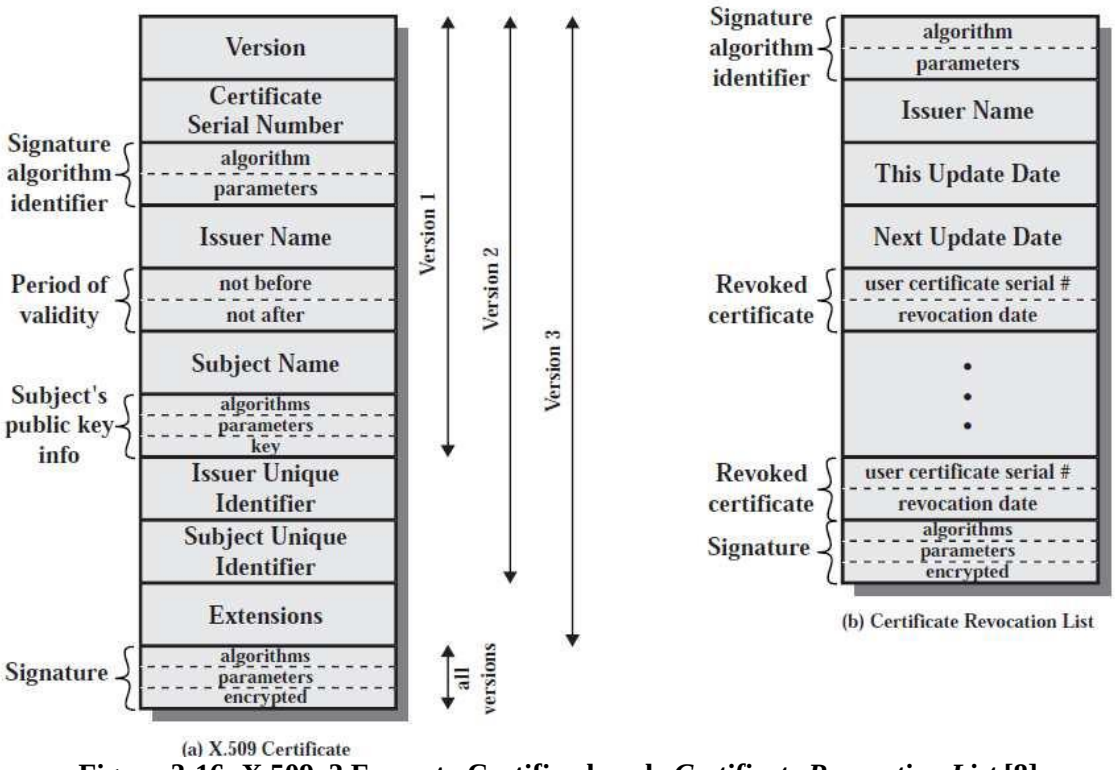

Figura 3-16: X.509v3 Formato Certificado e de *Certificate Revocation List* [8]

4. As normas IEEE 802.11 WLAN

4.1. Evolução e panorama histórico

A norma IEEE 802.11 pertence à família das normas 802, que foram desenvolvidas pelo IEEE para definir especificações para as redes locais e metropolitanas nos níveis físicos (PHY) e nível *data-link* (enlace ou ligação de dados - MAC) do modelo de referência OSI. Quando as redes sem fios começaram a ser concebidas, verificou-se logo que o meio físico tinha características diferentes devido a grandes atenuações, mesmo em pequenas distâncias, e à incapacidade de detectar colisões, pelo que o mecanismo CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*) da norma 802.3 não poderia ser utilizado.

Em 1997 o IEEE apresentou a primeira versão da norma IEEE 802.11, cujo objectivo era proporcionar conectividade de rede sem fios (*wireless*) entre diferentes dispositivos próximos (local). Esta norma descreve uma camada de controlo de acesso ao meio MAC (*Media Access Control*), e três camadas físicas distintas que permitiam uma taxa de transmissão de 1 Mbps ou 2 Mbps, duas baseadas em tecnologia de radio frequência (RF) - FHSS (*Frequency Hopping Spread Spectrum*) e DSSS (*Direct Sequence Spread Spectrum*) - na banda de frequência dos 2,4 GHz, e uma terceira baseada em infravermelhos.

De forma semelhante ao IEEE 802.3, o nível MAC funcionava de acordo com o princípio "escutar antes de falar", conhecido como DCF (*Distributed Coordination Function*) e implementado o mecanismo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), que em vez de detectar uma colisão (como acontece no IEEE 802.3), espera um intervalo de tempo definido (*backoff interval*) antes da transmissão de cada trama. A norma original especificava também um esquema opcional de acesso ao meio que dependia de uma unidade coordenadora central PCF (*Point Coordination Function*) que, através de mecanismos de "*poll*", permitia atribuir intervalos de tempo às estações.
Dois anos depois apareceu a primeira revisão da norma, referida como IEEE 802.11-1999, onde se apresentam duas extensões com novos esquemas de modulação que proporcionam velocidades de 5,5 Mbps ou 11 Mbps na banda de frequência dos 2,4 GHz (802.11b) e de velocidades de transmissão até 54 Mbps na banda de frequência dos 5 GHz (802.11a).
As observações efectuadas para as normas 802.11b, 802.11g e 802.11a apresentavam velocidades de transmissão de dados de cerca de metade da velocidade de transmissão no meio (Figura 4-8).

Em 2003 formou-se um grupo de trabalho (IEEE 802.11n)[1] para investigar a criação de um meio físico que pudesse proporcionar velocidades superiores a 100 Mbps, medidas na camada MAC.

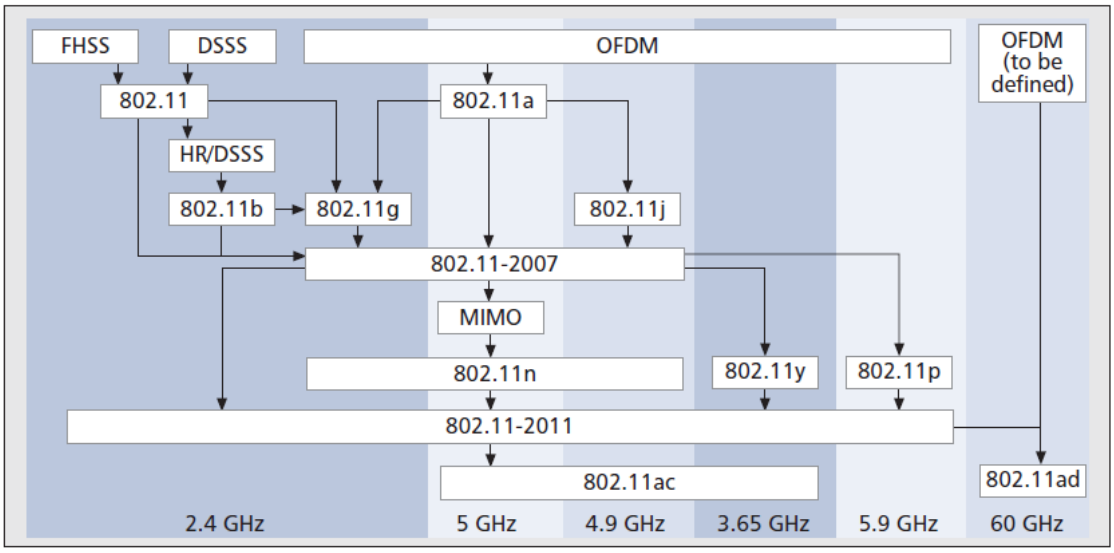

Figura 4-1: Evolução do nível físico 802.11 e suas dependências

A aprovação da norma 802.11n em 2009, veio trazer novas técnicas para aumento da velocidade de transmissão através da tecnologia MIMO (*Multiple Input/Multiple Output*) (Figura 4-2), que permite num único canal de rádio o suporte a múltiplos canais de dados, diferindo das normas anteriores em que tanto o emissor como o receptor utilizavam a tecnologia SISO (Single Input/Single Output). A norma 802.11n possibilita adicionalmente a utilização das duas bandas (2,4 GHz e 5 GHz) e a utilização de canais com 40 MHz em vez dos 20 MHz das normas anteriores (Figura 4-3).

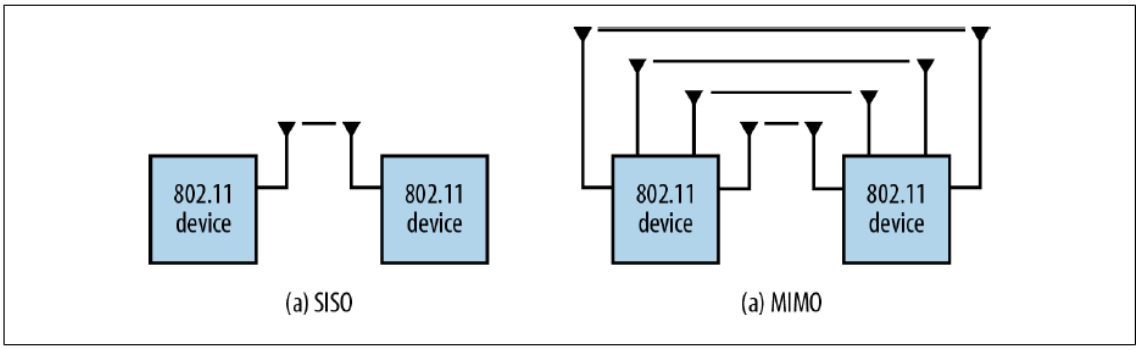

Figura 4-2: Comparação entre transmissão SISO e MIMO [4]

[1] As datas oficiais das normas e revisões então disponíveis na página oficial do site IEEE 802.11

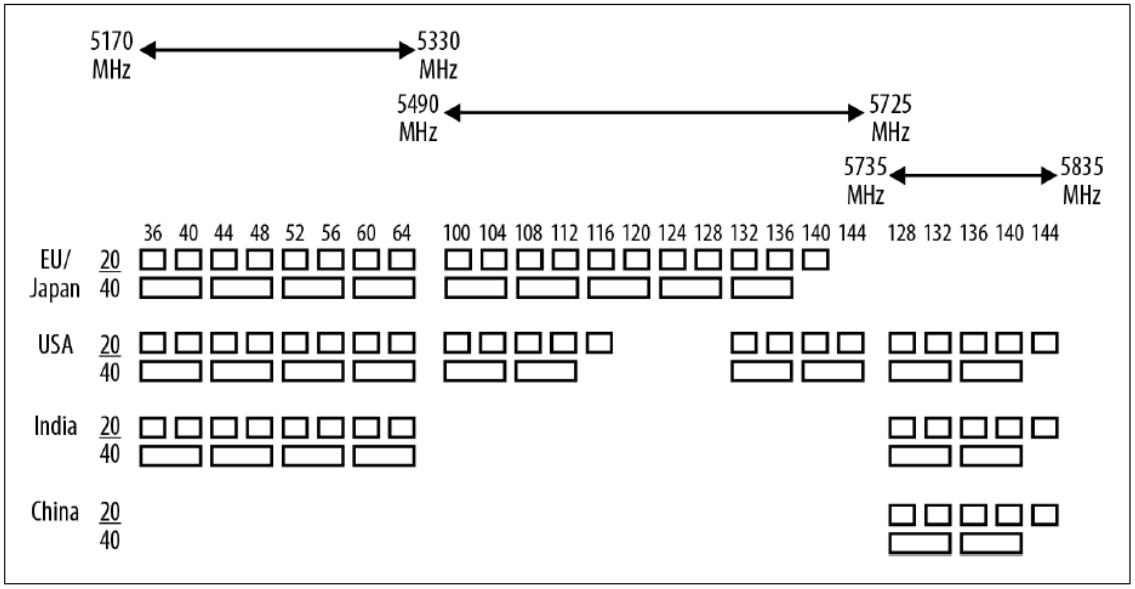

Figura 4-3: Mapa de canais disponíveis (5GHz) [4]

A norma IEEE 802.11ac, aprovada no final de 2013, veio permitir obter maiores velocidades de transmissão, superiores a 1 Gbps, maior escalabilidade no número de clientes associados a um AP (*access point*) e maior largura de banda por dispositivo. O aumento de velocidade (Figura 4-4) está associado a:

- Aumento do tamanho do canal de 40 MHz (802.11n) para os 80 MHz ou 160MHz.
- Modulação mais densa, utilizando uma modulação de amplitude em quadratura (265 QAM)
- Aumento de canais suportados na tecnologia MIMO (dos 4 canais máximos no 802.11n passa para o suporte de 8 canais no 802.11ac).

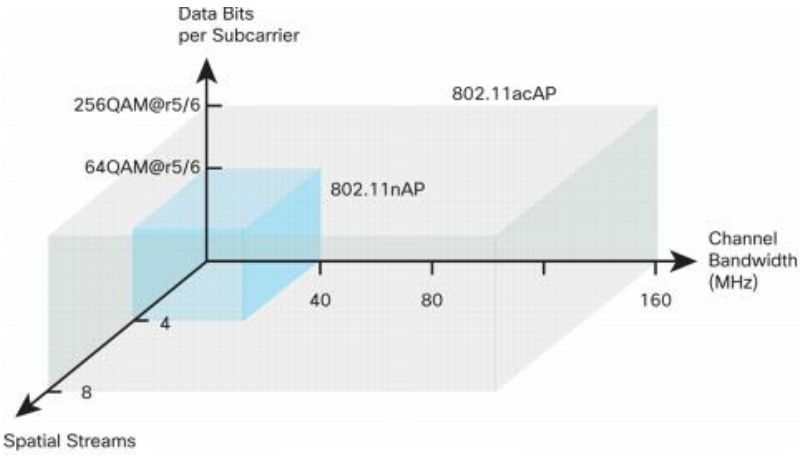

Figura 4-4: Vectores de melhoria de desempenho do 802.11ac

A norma 802.11ac permite desta forma disponibilizar taxas de transferência de dados conforme a Tabela 4-1 seguinte:

Tabela 4-1: Comparação de transmissão de dados de 802.11a, 11n, e 11ac

	Largura de Banda (MHz)	**Número de Canais Espaciais**	**Modulação e taxa de codificação**	**Intervalo de Guarda**	**Taxa de dados física (Mbps)**	**Débito (Mbps)***
802.11ª						
	20	1	64QAM r3/4	Long	54	24
802.11n						
Mínimo	20	1	64QAM r5/6	Long	65	46
Produtos de gama baixa (2,4 GHz only+)	20	1	64QAM r5/6	Short	72	51
Produtos gama média	40	2	64QAM r5/6	Short	300	210
Máximo definido	40	3	64QAM r5/6	Short	450	320
Máximo permitido	40	4	64QAM r5/6	Short	600	420
802.11ac wave 1						
Minimo	80	1	64QAM r5/6	Long	293	210
Produtos de gama baixa	80	1	256QAM r5/6	Short	433	300
Produtos de gama média	80	2	256QAM r5/6	Short	867	610
Produtos de topo de gama	80	3	256QAM r5/6	Short	1300	910
80 MHz máximo permitido	80	8	256QAM r5/6	Short	3470	2400
802.11ac wave 2						
Produtos de gama baixa	160	1	256QAM r5/6	Short	867	610
Produtos de gama média	160	2	256QAM r5/6	Short	1730	1200
Produtos de topo de gama	160	3	256QAM r5/6	Short	2600	1800
Produtos de ultra topo de gama	160	4	256QAM r5/6	Short	3470	2400

Máximo definido	160	8	256QAM r5/6	Short	6930	4900

4.1.1. Família de protocolos IEEE 802.11

Apresentam-se de seguida as normas relevantes para o estudo do IEEE 802.11:

802.11 – Norma original para redes sem fios (*Wireless*) designada por **"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications".** Foi inicialmente criada em 1997 e teve a sua primeira revisão em 1999. Esta norma especifica e define os mecanismos de funcionamento as WLAN cobrindo: o modelo de arquitecturas WLAN; vários serviços de como sejam associação, reassociação, autenticação e privacidade; formato das tramas (*frames*), incluindo as funcionalidades dos subníveis MAC e físico; as técnicas de modulação *Direct Sequence Spread Spectrum* (DSSS) e *Frequency Hopping Spread Spectrum* (FHSS), para transmissão a 1 Mbps e 2 Mbps na banda dos 2,4 GHz; e a utilização de WEP para componente de segurança.

802.11a – Norma para redes sem fios (Wireless) definida em 1999 e designado como **"High-Speed Physical Layer in the 5 GHz Band"** que especifica velocidades de transmissão até 54 Mbps, trabalhando na banda dos 5 GHz, com técnica de modulação OFDM.

802.11b – Norma para redes sem fios (Wireless) definida em 1999 e designado como **"Higher Speed Physical Layer Extension in the 2,4 GHz Band"** que acrescenta à norma original 802.11 velocidades de transmissão de 5 Mbps e 11 Mbps utilizando técnicas de modulação *Complementary Code Keying* (CCK) operando na banda dos 2,4 GHz.

802.11d – Norma definida em 2001 e designada como **"Amendment 3: Specification for operation in additional regulatory domains"**. Não sendo uma especificação de nível físico pretende adicionar mecanismos que permitam o funcionamento de produtos que cumpram a norma 802.11b em países nas diversas regiões do globo.

802.11e – Norma designada como **"Media Access Control (MAC) Quality of Service (QoS) Enhancements"**, acrescenta funcionalidades de qualidade de serviço (QoS) para as normas 802.11a, 802.11b e 802.11g, através da modificação do nível MAC.

802.11f – Norma definida em 2003 e designada por **"IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11™ Operation"**, que através do protocolo *inter-access point protocol* (IAPP) especifica as primitivas de serviço e protocolos que permitem a troca de informação entre dois pontos de acesso (*Access Point*) de quaisquer fabricantes. Este protocolo é opcional, mas permite a utilizador a mudança de APs num processo de *handover*.

802.11g – Norma definida em 2003 e designada por **"Extended Rate PHYs",** permite o funcionamento de dispositivos com velocidades de transmissão até 54 Mbps na banda dos 2,4Ghz. Permite a utilização de modulação OFDM, modulação *packet binary convolution coding* (PBCC) e a modulação *complementary code keying* (CCK) já utilizada na norma 802.11b.

802.11h – Norma definida em 2003 e designada por **"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Spectrum and Transmit Power Management Extensions in the 5GHz band in Europe"**, define o modelo de gestão dinâmica da potência de transmissão e da selecção dinâmica da frequência no funcionamento de dispositivos 802.11a para a Europa.

802.11i – Norma definida em 2004 e designada por **"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications--Amendment 6: Medium Access Control (MAC) Security Enhancements"**, pretende adicionar aos standards 802.11 um conjunto novo de funcionalidades de segurança, possibilitando mecanismos de autenticação, de cifra por blocos AES (*Advanced Encryption Standard*) ao invés de RC4 utilizado no WEP e WPA.

802.11n – Norma definida em 2009 e designada por **"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Enhancements for Higher Throughput"**, vem adicionar à norma 802.11 um conjunto de alterações ao nível físico e de controlo de acesso ao meio (MAC), como seja o MIMO, possibilitando a melhoria das velocidades de transmissão de 54 Mbps para um máximo de 600 Mbps.

802.11ac – Norma definida em Dezembro 2013 e designada por **"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment: Enhancements for Very High Throughput for operation in bands below 6 GHz"**, pretende

adicionar à norma 802.11 um conjunto de alterações ao nível físico e de controlo de acesso ao meio (MAC) que disponibilizem modos de operação capazes de suportar velocidades de transmissão de dados superiores a 1 Gbps para multi estações ou de 500 Mbps para uma estação e manter compatibilidade com normas IEEE 802.11 anteriores na banda do 5 GHz.

802.15– Norma para redes sem fios pessoal (WPAN) que funciona na banda de frequência dos 2,4 GHz baseado na especificação Bluetooth v1.1. O Bluetooth tem uma potência de emissão reduzida e uma cobertura reduzida (na ordem dos metros) sendo utilizado em equipamentos pessoais como sejam telemóveis, PDAs, computadores e impressoras.

802.16 – Norma original para redes metropolitanas sem fios - "*Broadband Wireless Metropolitan Area Network* (BWMAN) - para funcionarem em frequências dos 10 aos 66 GHz.

802.16a – Norma definida em 2003 e designada **"Amendment 2: Medium Access Control Modifications and Additional Physical Layer Specifications for 2-11 GHz"** original para redes metropolitanas sem fios - *Broadband Wireless Metropolitan Area Network* (BWMAN) - para funcionarem em frequências dos 2 aos 11 GHz e com modulações OFDM e OFDMA.

802.1x – Norma designada por "**Local and Metropolitan Area Networks: Port-Based Network Access Control".** Mecanismo robusto de autenticação em redes.

4.2. Os níveis do IEEE 802.11

A norma IEEE 802.11 adere à arquitectura genérica de redes IEEE 802, estando posicionada no modelo de referência *Open System Interconnection* (OSI) no nível enlace (*Data Link Layer)* na componente de acesso ao meio (MAC) e no nível Físico (PHY) (Figura 4-6).

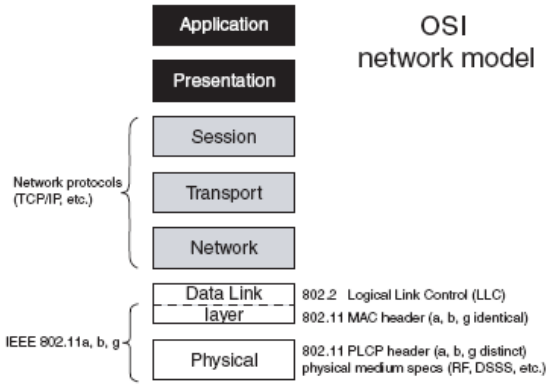

Figura 4-5: Posicionamento do IEEE 802.11 no modelo OSI.

Esta arquitectura permite um interface transparente, através da camada LLC (Logical Link Control), especificado na norma IEEE 802.2 (Figura 4-5), com os níveis superiores, mesmo quando há movimento das estações por alterações de características de meio. Permite-se assim que protocolos de rede (tal como o IP) funcionem sobre IEEE 802.11 WLAN sem alterações, tal como se fossem implementados sobre redes Ethernet em cabo.

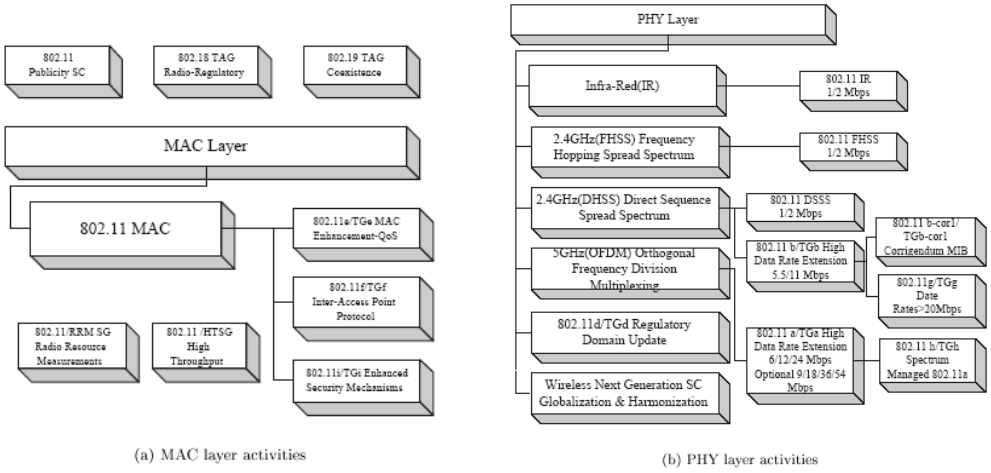

Figura 4-6: Framework dos níveis MAC e Físico do IEEE 802.11

4.3. O nível físico IEEE 802.11

Ao nível físico, a norma IEEE 802.11 apresentava em 1997 três opções de implementação na banda dos 2,4 GHz. Os três níveis físicos (PHY) são o Infravermelho (IR), a transmissão rádio *Frequency Hopping Spread Spectrum* (FHSS) e a transmissão rádio *Direct Sequence Spread Spectrum* (DSSS). Todos os três níveis suportam o funcionamento a 1 e 2 Mbps. Em resultado

do trabalho dos grupos *IEEE Working Group A e B*, em 1999 o IEEE publicou as normas IEEE 802.11a e IEEE 802.11b.

O IEEE 802.11a funciona na banda do 5 GHz, "*unlicensed national information infrastructure*" (U-NII) usando a transmissão rádio *Orthogonal Frequency Division Multiplexing* (OFDM) disponibilizando as velocidades de 6, 9, 12, 24, 36, 48 e 56 Mbps. As velocidades 6, 12, e 24 Mbps, são obrigatórias em qualquer implementação 802.11ª, sendo os 6 e o os 12 Mbps, virtualmente idênticas às velocidades de 5,5 e 11 Mbps do IEEE 802.11b.

O IEEE 802.11b funciona na banda dos 2,4 GHz usando DSSS (com codificação *Binary Phase Shift Keying* (BPSK) para 1 Mbps e *Quadrature Phase Shift Keying* (QPSK) para os 2, 5,5 e 11 Mbps), funcionando nas velocidades de 1, 2, 5,5 e 11 Mbps.

O IEEE 802.11g, ratificado em Junho de 2003, funciona nas mesmas velocidades e tecnologia OFDM que o IEEE 802.11a, mantendo também a compatibilidade de velocidade e banda (2,4GHz) utilizados no IEEE 802.11b.

	802.11a	802.11b	802.11g
Operating frequencies	5 GHz U-NII/ISM Bands	2.4 GHz ISM Band	2.4 GHz ISM Band
FCC regulation	Part 15.407/15.247	Part 15.247	Part 15.247
Modulation techniques	OFDM	Barker Code/CCK	Barker Code/CCK/OFDM
Data rates (Mbps)	6,9,12,18,24,36,48,54	1,2,5.5,11	1,2,5.5,11 6,9,12,18,24,36,48,54
Slot time	9 □s	20 □s	20 □s 9 □s (optional)
Preamble	OFDM	Long Short (optional)	Long/Short/OFDM

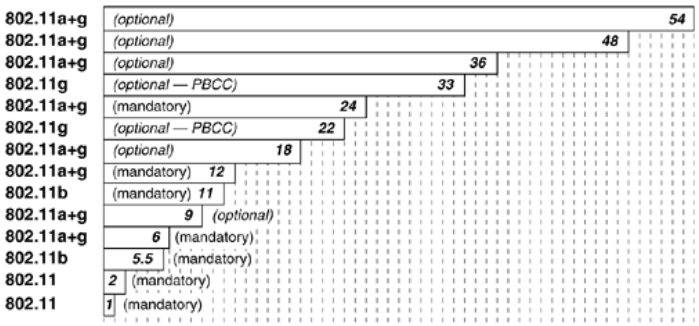

Figura 4-7: Parâmetros de transmissão em IEEE 802.11.

Quando estão presentes nós 802.11b, os nós 802.11g utilizam mecanismos de acesso ao meio *Request-To-Send/Clear-To-Send* (RTS/CTS) ou só CTS por cada transmissão, tendo como resultado uma redução do débito de transmissão do nó.

	Number of Non-Interfering Channels	Modulation	Maximum Link Rate	Theoretical Maximum TCP Rate	Theoretical Maximum UDP Rate
802.11b	3	CCK	11 Mbps	5.9 Mbps	7.1 Mbps
802.11g (with 802.11b)	3	OFDM/CCK	54 Mbps	14.4 Mbps	19.5 Mbps
802.11g (11g-only mode)	3	OFDM/CCK	54 Mbps	24.4 Mbps	30.5 Mbps
802.11a	19[1]	OFDM	54 Mbps	24.4 Mbps	30.5 Mbps
802.11a Atheros Turbo Mode™	6	OFDM	108 Mbps	42.9 Mbps	54.8 Mbps

1 13 non-overlapping channels in the United States and up to 19 non-overlapping channels in Europe depending on local regulations.

Figura 4-8: Velocidade máxima teórica de transmissão (c/pacotes de 1.500 bytes).

4.3.1. Regulamentação de frequências

A regulação do espectro de rádio frequência é efectuada em cada país, no entanto existem alguns organismos internacionais, com sejam o *International Telecommunication Union* (ITU), que tentam harmonizar a utilização do espectro nas três grandes áreas . Europa, Ásia e América do Norte. Existem vários níveis físicos que poderão ser utilizados no contexto das WLANs IEEE 802.11. As opções advêm do facto de haver diversos meios físicos através dos quais poderão ser transmitias as tramas (*frames*), entre os quais bandas de infravermelhos ou bandas de rádio nas frequências dos 2,4 GHz (2.450 ± 0.050 GHz, com uma largura de banda de 100 MHz) e dos 5GHz. As frequências e canais utilizados no IEEE 802.11 poderão não estar disponíveis em todos os países pelo que poderá não ser garantido o funcionamento de alguns canais em alguns países.

4.3.2. Frequências e canais utilizados no IEEE 802.11

Os níveis físicos definidos no IEEE 802.11 permitem a utilização de várias combinações de frequências válidas e as modulações de sinal associadas para que se possa atingir as velocidades de transmissão definidas. Algumas das combinações são obrigatórias e outras são opcionais, tal como descrito na figura seguinte.

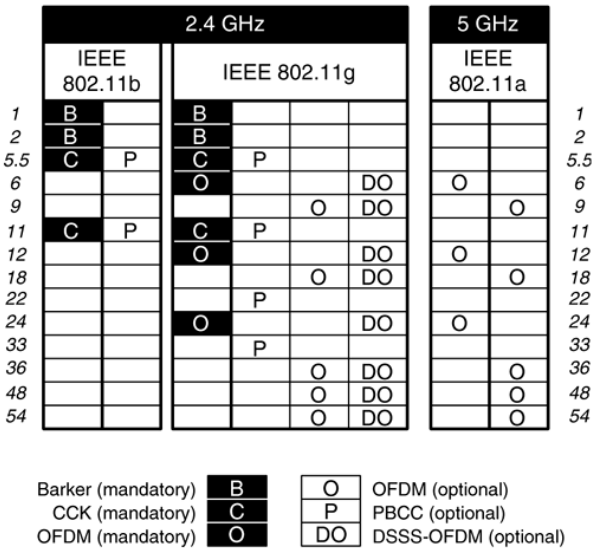

Figura 4-9: Parâmetros de funcionamento do IEEE 802.11

Para ultrapassar problemas como a degradação do sinal rádio, os nós 802.11 WLAN podem reduzir para o escalão anterior a sua velocidade de transmissão, bem como regressar aos escalões seguinte quando a qualidade do sinal o permitir. A detecção da qualidade do sinal é obtida através de um dado contido no protocolo, chamado de *Received Signal Strength Indicator* (RSSI) e normalmente expresso em decibéis (dB).

4.3.3. Normas IEEE 802.11b e IEEE 802.11g

Apesar de utilizarem diferentes métodos de modulação do sinal, ambas as normas usam a gama de frequências de 2.400 MHz a 2.483,5 MHz. Estão definidos na norma 14 canais espaçados de 5 MHz, começando no 2.412 MHz e terminando nos 2.472 MHz para os primeiros 13 canais. Não foram definidos canais centrados nos 2.477 MHz e 2.482 MHz, ficando o canal 14 definido na frequência 2.484 MHz (2 MHz superiores ao esperado) e apenas utilizado no Japão. Cada um dos canais utiliza uma largura de banda de 22 MHz centrado na frequência do canal, pelo que o canal 1 funciona no intervalo entre 2.401MHz e 2.423MHz, (centrado nos 2.412MHz), o canal 2 estará sobreposto quase por completo o canal 1, funcionando no intervalo entre 2.406MHz e 2.428MHz, (centrado nos 2.417MHz), e assim sucessivamente para os outros canais. Como poderemos observar poderemos ter no máximo 3 canais que não interferem entre si (3x22Mhz em 84MHz) e que correspondem aos canais 1, 6 e 11.
As seguintes figuras (Figura 4-10 e Figura 4-11) sintetizam as frequências centrais e larguras de banda associadas a cada canal.

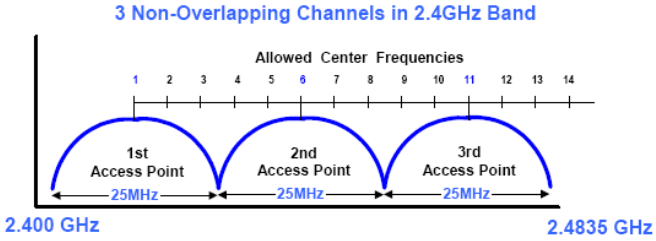

Figura 4-10: Canais sem sobreposição (1, 6, 11).

	Low	Center	High		0x10 (FCC)	0x20 (IC)	0x30 (ETSI)	0x31 Spain	0x32 France	0x40 Japan	0x41 Japan	
1	2401	**2412**	2423	1	X	X	X				X	1
2	2406	**2417**	2428	2	X	X	X				X	2
3	2411	**2422**	2433	3	X	X	X				X	3
4	2416	**2427**	2438	4	X	X	X				X	4
5	2421	**2432**	2443	5	X	X	X				X	5
6	2426	**2437**	2448	6	X	X	X				X	6
7	2431	**2442**	2453	7	X	X	X				X	7
8	2436	**2447**	2458	8	X	X	X				X	8
9	2441	**2452**	2463	9	X	X	X				X	9
10	2446	**2457**	2468	10	X	X	X	X	X		X	10
11	2451	**2462**	2473	11	X	X	X	X	X		X	11
12	2456	**2467**	2478	12			X		X		X	12
13	2461	**2472**	2483	13			X		X		X	13
n/a	2466	2477	2488	n/a								
n/a	2471	2482	2493	n/a								
14	2473	**2484**	2495	14						X		14

Figura 4-11: Canais IEEE 802.11b/g na banda dos 2,4 GHz

4.3.4. Norma IEEE 802.11a

O IEEE 802.11a trabalha na banda dos 5 GHz. Nos EUA a FCC (entidade reguladora) reservou inicialmente 3 intervalos de largura de banda com especificações diferentes quanto à potência de emissão definidas como U-NII (*Unlicensed National Information Infrastructure*), correspondentes às frequências 5150-5250 MHz, 5250-5350 MHz e 5725-5825 MHz. O intervalo 5150-5250 MHz da banda U-NII tem o limite de potência mais restritivo, e tem como objectivo a utilização em aplicações de pequenas distancia ou zonas interiores (WLANs). A potência é limitada de maneira a evitar que os periféricos interfiram com o funcionamento dos serviços de satélite.

O intervalo 5250-5350 MHz da banda U-NII tem limites mais reduzidos na potência de radiação, sendo o mais aconselhado para a utilização dentro e entre edifícios. O terceiro intervalo, 5725-5825 MHz, é o menos restritivo em termos de potência, permitindo funcionamento em distâncias maiores (alguns quilómetros) quando o sinal é emitido por antenas direccionais.

Definição de canais na banda U-NII

A norma IEEE 802.11a define 200 canais espaçados de 5 KHz, entre os 5 GHz e os 6 GHz (Figura 4-12). Por exemplo, o canal 40 começa nos 5200 MHz e o canal 41 nos 5205 MHz.
A norma IEEE 802.11a especifica que deverá haver um intervalo de 30 MHz no início e outro no fim da banda U-NII 5150-5350 MHz que não deverão ser utilizados. Tal como mostrado na figura 8, os restantes 140 MHz do espectro na banda mais baixa do U-NII pode conter 8 canais não sobrepostos de 20 MHz cada, sendo a distância entre canais de 20 MHz. O mesmo acontece com a banda mais alta do U-NII, onde se podem obter mais quatro canais não sobrepostos, perfazendo um total de 12 canais não sobrepostos.

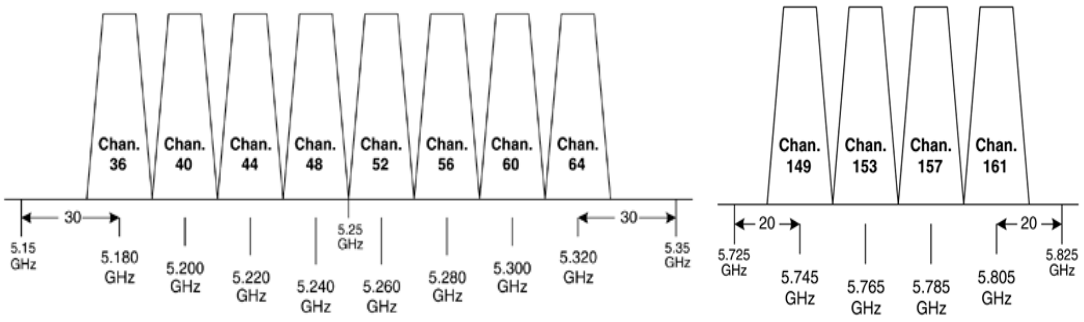

Figura 4-12: Canais IEEE 802.11a na banda dos 5 GHz

4.3.5. Norma IEEE 802.11n

A norma 802.11n pode utilizar ambas as bandas de 2,4 GHz e 5 GHz (Figura 4-3). Das alterações introduzidas nesta norma deve salientar-se a tecnologia MIMO que permite que num único canal rádio a emissão de múltiplos canais (*streams*) de dados em simultâneo. Antes do 802.11n o emissor e o receptor apenas poderiam manter um canal de dados (*stream*) no canal de rádio (SISO) funcionando num modelo *half-duplex*. Num sistema MIMO, ambos, emissor e receptor, poderão estar a enviar dados, de forma independente e em simultâneo (Figura 4-13). O 802.11n utiliza técnicas de modulação OFDM (já utilizadas no 802.11a/g) para cada caminho, possibilitando um máximo de 4 canais espaciais (Figura 4-14).

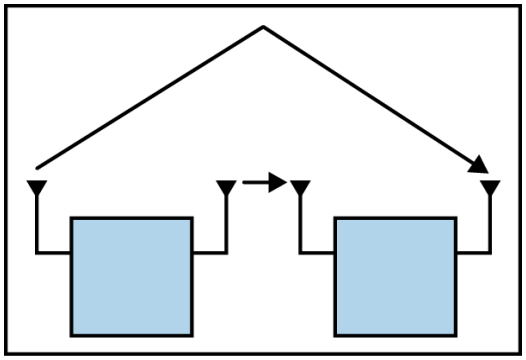

Figura 4-13: Criação de múltiplos canais espaciais

Um outro factor que permitiu aumentar para o dobro a velocidade de transmissão consistiu na possibilidade de utilização de canais de 40 MHz (para além de canais de 20 MHz) [4].

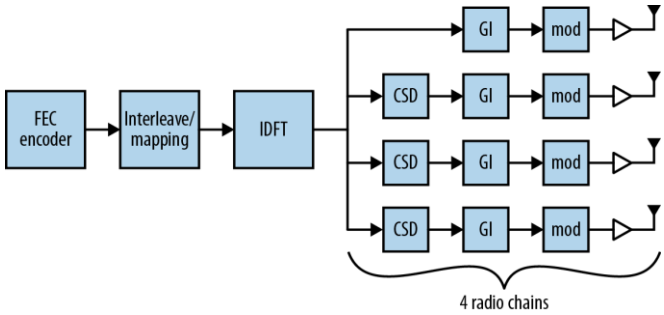

Figura 4-14: Diagrama de blocos de um interface 802.11n 4x4

A definição dos vários esquemas de modulação que podem ser utilizados está definida na Tabela 4-2 seguinte:

Tabela 4-2: Esquemas de modulação em 802.11n, velocidade de transmissão

MCS Index	Modulation	Coding Rate	Spatial Streams	802.11n Data Rate (Mbps)			
				20-MHz		40-MHz	
				L-GI	S-GI	L-GI	S-GI
0	BPSK	1/2	1	6.5	7.2	13.5	15
1	QPSK	1/2	1	13	14.4	27	30
2	QPSK	3/4	1	19.5	21.7	40.5	45
3	16-QAM	1/2	1	26	28.9	54	60
4	16-QAM	3/4	1	39	43.3	81	90
5	64-QAM	2/3	1	52	57.8	108	120
6	64-QAM	3/4	1	58.5	65	122	135
7	64-QAM	5/6	1	65	72.2	135	150
8	BPSK	1/2	2	13	14.4	27	30
9	QPSK	1/2	2	26	28.9	54	60
10	QPSK	3/4	2	39	43.3	81	90
11	16-QAM	1/2	2	52	57.8	108	120
12	16-QAM	3/4	2	78	86.7	162	180
13	64-QAM	2/3	2	104	116	216	240
14	64-QAM	3/4	2	117	130	243	270
15	64-QAM	5/6	2	130	144	270	300
16	BPSK	1/2	3	19.5	21.7	40.5	45
17	QPSK	1/2	3	39	43.3	81	90
18	QPSK	3/4	3	58.5	65	121.5	135
19	16-QAM	1/2	3	78	86.7	162	180
20	16-QAM	3/4	3	117	130	243	270
21	64-QAM	2/3	3	156	173.3	324	360
22	64-QAM	3/4	3	175.5	195	364.5	405
23	64-QAM	5/6	3	195	216.7	405	450
24	BPSK	1/2	4	26	28.9	54	60
25	QPSK	1/2	4	52	57.8	108	120
26	QPSK	1/2	4	78	86.7	162	180
27	16-QAM	1/2	4	104	115.6	216	240
28	16-QAM	3/4	4	156	173.3	324	360
29	64-QAM	2/3	4	208	231.1	432	480
30	64-QAM	3/4	4	234	260	486	540
31	64-QAM	5/6	4	260	288.9	540	600

4.3.6. Norma IEEE 802.11ac

A norma 802.11ac define que deverá trabalhar na banda do 5 GHz, evitando desta forma as interferências que existem na banda do 2,4 GHz (incluindo dispositivos Bluetooth, microondas, etc.) e a reduzida largura de banda ai disponível (80 MHz). A utilização de modulação 256 QAM, a utilização de tecnologia *multi-user* MU-MIMO que permite a um AP transmitir múltiplas tramas para múltiplos clientes ao mesmo tempo e sobre o mesmo espectro de frequências, a utilização de canais de 80 MHZ ou 160 MHz (Figura 4-15) e mais canais espaciais (8 no caso do 802.11ac versus 4 no 802.11n) permitiu um aumento significativo na velocidade de transferência de dados (Tabela 4-1).

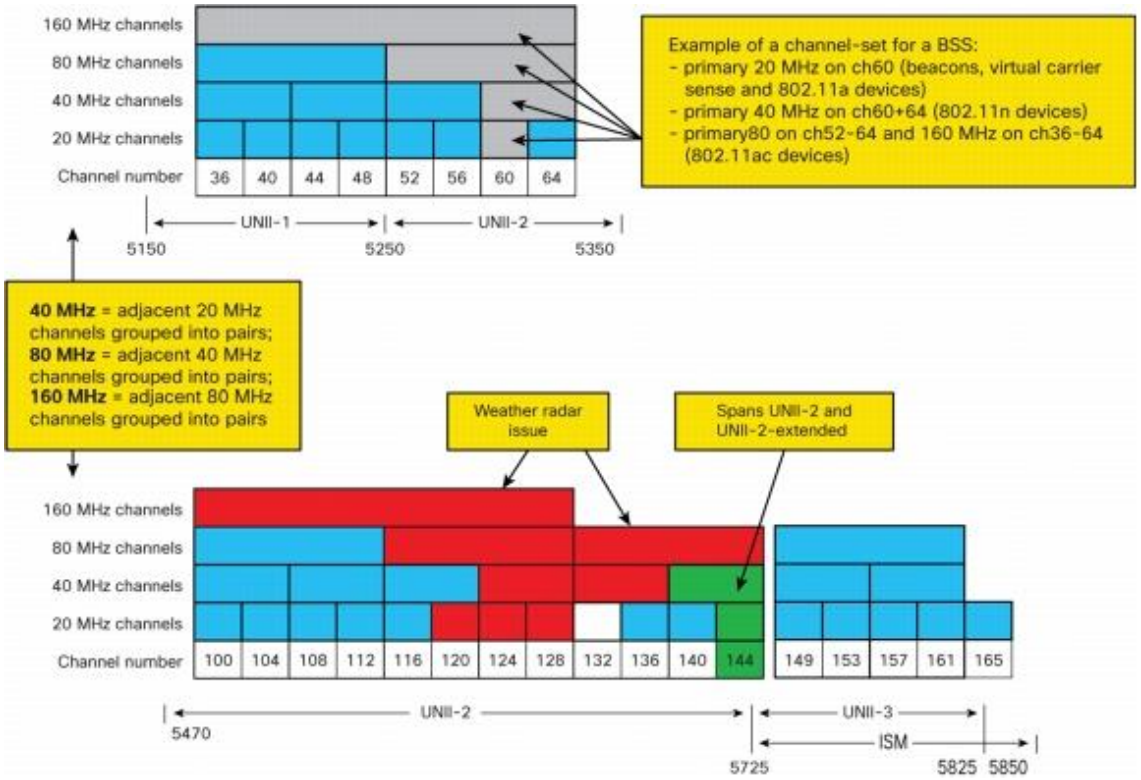

Figura 4-15: Agregação de canais no IEEE802.11ac

4.3.7. Medidas de sinal e ruído

Para medir a energia eléctrica das ondas de rádio usadas no IEEE 802.11 utiliza-se a unidade de potência Watt, e no caso das WLAN especificamente o mili-Watt (mW). As potências máximas de emissão nas WLAN estão normalizadas para cada banda (900Mhz – 800mW, 2.4GHz-125mW e nos 5GHz [5150/5250Mhz-50 mW; 5250/5350MHz-250mW;5725/5825Mhz-1W]).

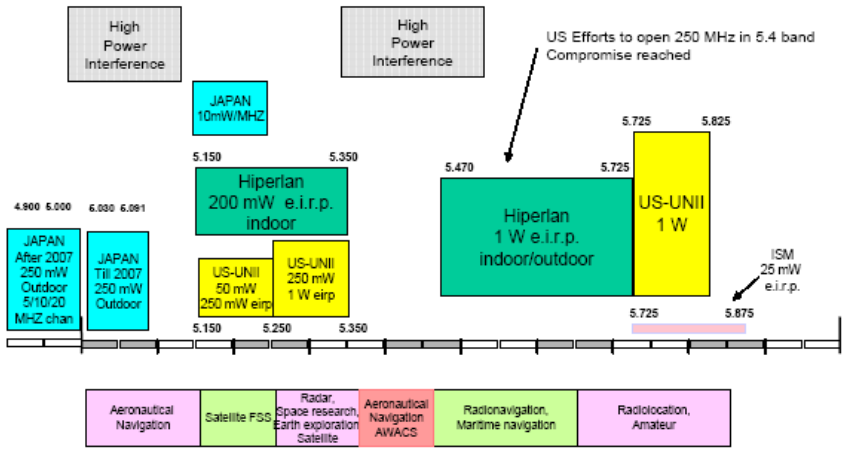

Figura 4-16: Distribuição de frequências e potências máximas.

Como a energia detectada no receptor é inferior em várias ordens de magnitude, utiliza-se a notação *decibel mili-Watt* (dBm) para expressar as medidas de potência. O decibel representa uma relação entre duas potências e expressa pela seguinte fórmula dB = 10.log (P2/P1) e no caso particular da WLAN para calcular dBm = 10 log (Potência em Watts) + 30. Poderemos ver que 1 Watt =+30 dBm ou que 0dBm = 1mW e que podemos expressar por exemplo a potência de emissão de uma estação de 32 mW em 15dBm. É também através desta medida que expressamos as atenuações de sinal provocadas por distâncias ou obstáculos.

4.3.8. Interferência de canais adjacentes

A escolha dos canais a utilizar em cada AP durante o dimensionamento é fundamental para garantir o bom funcionamento de uma rede sem fios. A interferência entre os AP provocada pela utilização de canais adjacentes pode provocar atrasos e a perda de comunicações e este efeito é resumido na seguinte figura.

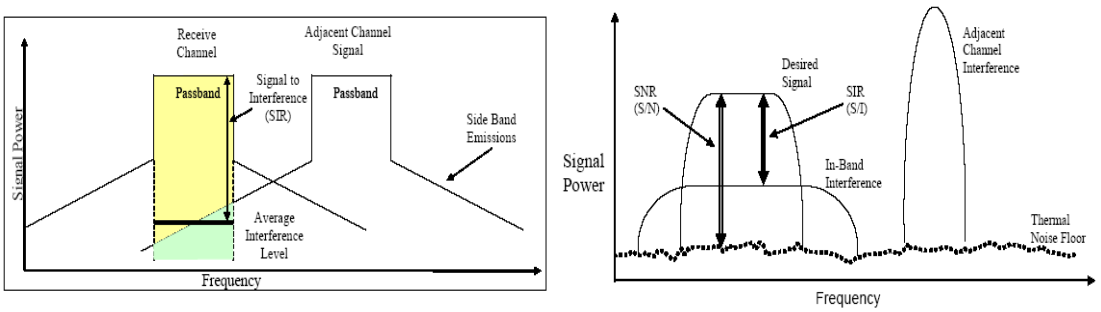

Figura 4-17: Interferência entre canais adjacente.

O desempenho da rede sem fios pode ser medido através da relação *Signal-to-Interference Ratio* (SIR). Os fenómenos de interferência podem ser provocados pelos canais adjacentes ou por outras fontes como sejam terminais Bluetooth ou equipamentos microondas.

4.4. Topologias WLAN

A norma define três topologias base para as WLAN: *Independent Basic Service Set* (IBSS), *Basic Service Set* (BSS) e o *Extended Service Set* (ESS). Estas topologias são implementadas através de dois modos de funcionamento, o modo ***ad hoc*/IBSS** e o modo ***infrastructure***.

4.4.1. Modo de funcionamento *Ad Hoc/Independent Basic Service Set*

A norma proporciona mecanismos para a criação de redes simples constituídas apenas por estações *wireless* sem necessidade de utilizarem AP. Uma utilização típica destas redes é a ligação entre estações para troca de ficheiros ou caso uma das estações tenha ligação a uma LAN poder servir de *bridge* entre as estações wireless e a LAN. A este modelo chama-se ligação ***ad hoc*** e a norma refere esta topologia como sendo *Independent Basic Service Set* (IBSS).

4.4.2. Modo de funcionamento de *Infrastructure*

Este modo caracteriza-se por termos uma rede com pelo menos um AP ligado à infra-estrutura de rede física (*wired*) e que interliga um conjunto de estações. Este modelo simples é chamado de *Basic Service Set* (BSS) e todas as comunicações entre estações passam através do AP, bem como as comunicações com serviços especializados (servidores de ficheiros, servidores de impressão, links Internet). Um *Extended Service Set* (ESS) é um conjunto de dois ou mais BSS interligados fisicamente por cabo (*wired*) ou por rádio (*Wireless*) - Figura 4-18. O IEEE 802.11 suporta configurações onde múltiplas células (BSS) utilizam o mesmo canal, no entanto para evitar interferências devem utilizar-se canais diferentes (*non-overlapping*).

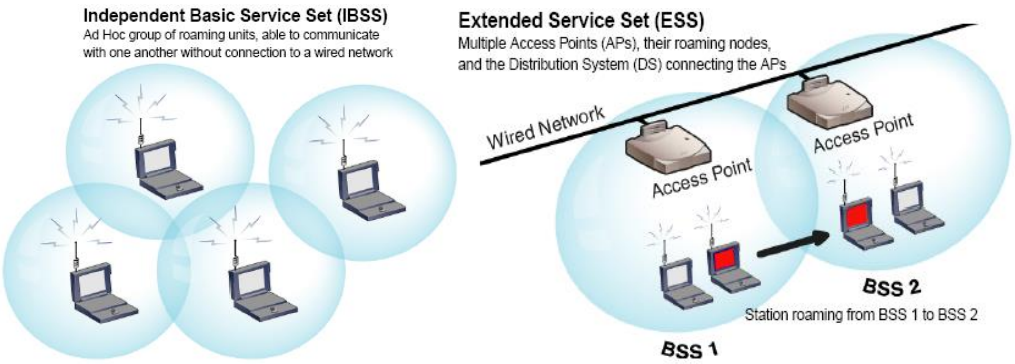

Figura 4-18: Topologias IBSS, BSS e ESS.

4.5. A estrutura das tramas do IEEE 802.11 MAC Sub-layer

Descreve-se agora a estrutura das tramas (*frames*) do protocolo no *sub-layer MAC.*

Uma das operações mais importantes realizadas pelo *sub-layer MAC* do nível enlace (*Data Link*) é conhecida por "*framing*", e consiste no processo de encapsular os pacotes provenientes

de um nível superior num conjunto de vários pacotes aos quais são adicionados *headers* e *trailers* do subnível MAC. O "*framing*" inclui a definição do interface com o nível físico.

O *header* do nível *Data Link* deve incluir pelo menos os seguintes três elementos:

- MAC sub-layer Destination Address (MAC-DA)
- MAC sub-layer Source Address (MAC-SA)
- Informação para identificar o descritor do protocolo de nível superior (identificado no *LLC sub-layer*, identificado pelo protocolo *LLC sub-layer* ou pelo protocolo *LLC sub-layer* em conjunto com o *Sub-Network Access Protocol* (SNAP))

Os dois primeiros itens são itens do subnível MAC, e o terceiro é frequentemente encontrado na forma de um campo "*Type*" ou "*Protocol*", que indica o tipo de pacote do nível superior que está dentro da trama.

O protocolo do IEEE 802.2 *LLC sub-layer* proporciona uma forma limitada de demultiplexagem para os protocolos superiores através dos seus campos *Destination and Source Service Access Point (DSAP and SSAP)*. Devido à limitação do número de LLC SAP, existe outro protocolo no *LLC sub-layer* conhecido como *Subnetwork Access Protocol (SNAP)*, que contém o campo "*Type*" de dois bytes e que se encontra posicionado por cima do protocolo LLC.

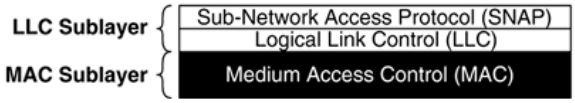

Figura 4-19: LLC e MAC sub-layers versus protocolos MAC, LLC, e SNA.

4.5.1. Formato geral das tramas IEEE 802.11

As tramas do *MAC sub-layer* são descritas como uma sequência de campos numa determinada ordem fixa. O formato geral das tramas está apresentado na Figura 4-20, sendo que os campos *Address1, Address2, Address3, Sequence Control, Address4 e Frame Body* só aparecem em algumas tramas.

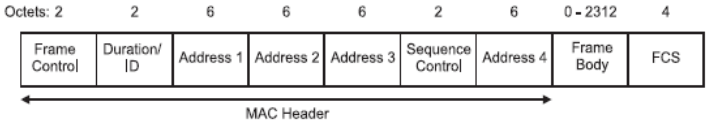

Figura 4-20: Formato geral das tramas do sub-layer MAC.

Existem três tipos de tramas dependendo da informação contida no campo *Frame Control* e que são: Trama de Controlo (*Control Frame*), trama de gestão (*Management Frame*) e trama de dados (*Data Frame*). Uma das partes mais importantes do cabeçalho (*header)* MAC é a informação de endereçamento que será descrita num dos pontos seguintes.

4.5.2. Campo *Frame Control* das tramas IEEE 802.11

Todas as tramas IEEE 802.11 começam com o campo *Frame Control* (FC) com tamanho de 2 bytes, cuja estrutura se apresenta na figura 13.

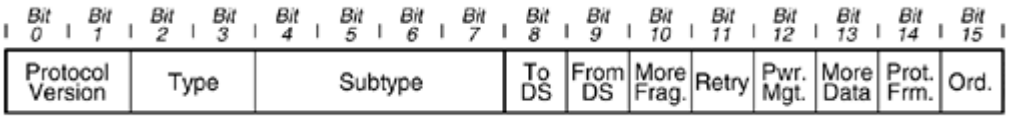

Figura 4-21: Campo Frame Control do IEEE 802.11.

Descrição da função de cada subcampo do *Frame Control*:

- O campo *Protocol Version* (bits 0 e 1) definido pelo IEEE 802.11 de 1999 tem o valor "0x00".
- Os campos "*Type"* (bits 2 e 3) e "*Subtype"* (bits 4 até ao 7) definem o formato da trama que segue o campo FC (Frame Control) e estão definidos na Figura 4-22.

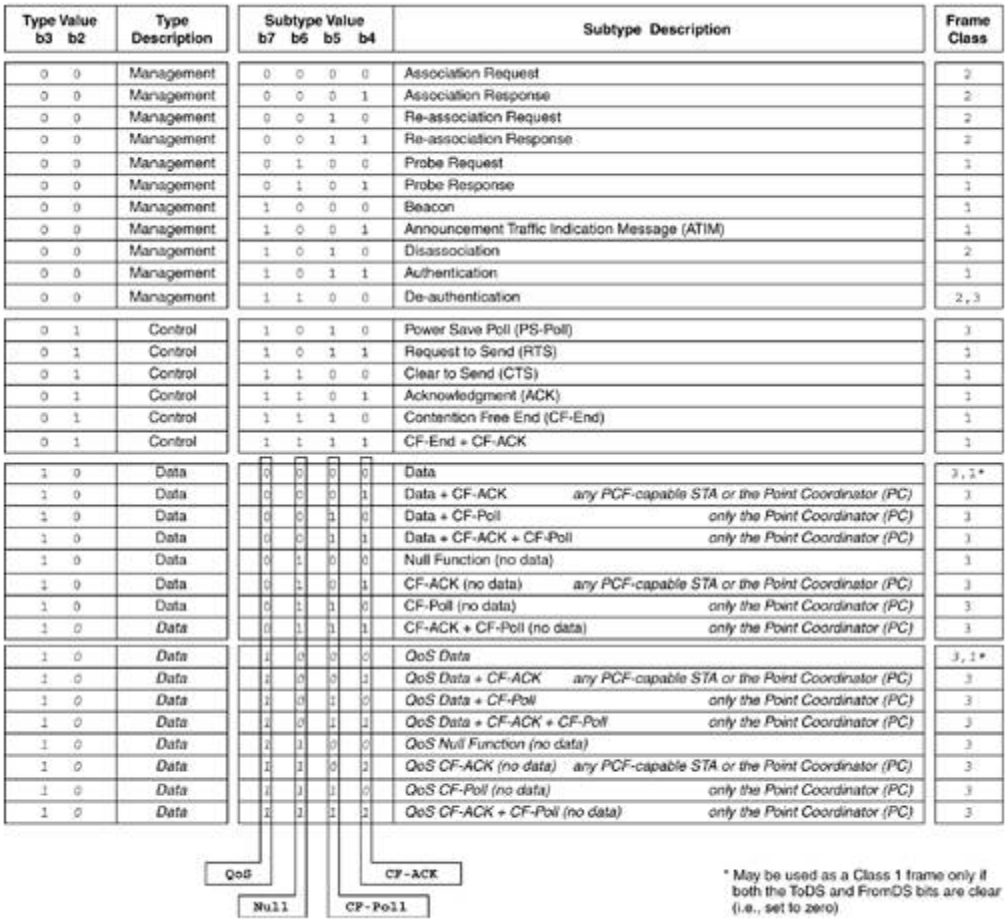

Figura 4-22: Tramas de gestão, controlo e de dados do IEEE 802.11.

O campo "*Type*" permite a definição de um total de quarto tipos de tramas IEEE 802.11, dos quais três foram inicialmente definidos na norma IEEE 802.11 de 1999:

- Bit 3 (0) + Bit 2 (0)— *Management*
- Bit 3 (0) + Bit 2 (1)— *Control*
- Bit 3 (1) + Bit 2 (0)— *Data*
- Bit 3 (1) + Bit 2 (1)— Não definido

Através da utilização do campo "*Subtype"* de 4 bits, cada um dos tipos de trama pode conter até 16 subtipos. Quando o campo "*Type"* indica uma trama de dados (*Data*), cada um dos quatro bits do campo "*Subtype"* tem um significado particular, enquanto que se for uma trama de *Management* ou *Control* o campo "*Subtype"* é apenas um numérico sem estrutura.

- Os campos "*ToDS"* (bit 8) e "*FromDS"* (bit 9) são colocados a "1" quando as tramas do tipo *Data* respectivamente se destinam ou são recebidas do *Distribution System*, e a "0" nas outras tramas.

As combinações permitidas para estes campos são as seguintes:

To/From DS values	Meaning
To DS = 0 From DS = 0	A data frame direct from one STA to another STA within the same IBSS, as well as all management and control type frames.
To DS = 1 From DS = 0	Data frame destined for the DS.
To DS = 0 From DS = 1	Data frame exiting the DS.
To DS = 1 From DS = 1	Wireless distribution system (WDS) frame being distributed from one AP to another AP.

Figura 4-23: Campos *ToDS/FromDS* em tramas de *dados* do IEEE 802.11.

- O campo "*More Frag*." (i.e., *More Fragments*) (Bit 10), se for colocado a "1" indica que a trama do tipo *Management* ou *Data* é um fragmento de um MSDU ou MMPDU. Se este bit for colocado a "0" então esta trama é o último fragmento de um MSDU ou então a trama nunca foi segmentada. Quando uma estação (STA) efectua uma fragmentação, cada fragmento do MSDU ou MMPDU é transmitido ordenadamente, e é recebido um *acknowledge* de cada fragmento antes de ser enviado o novo fragmento.
- O campo "*Retry*" (bit 11), é colocado a "1" quando o MPDU ou MMPDU corrente é uma retransmissão de um MPDU ou MMPDU anterior, permitindo a detecção e eliminação de tramas duplicadas.
- O campo "*Pwr. Mgt.*" (i.e., *Power Management*) (bit 12), é utilizado para indicar para que estado de funcionamento vai transitar depois de enviar o MPDU corrente. Quando uma STA activa este bit, notifica que depois do envio da trama e da recepção do ACK vai passar para modo "*power-save*", em vez de se manter no estado activo.
- O campo "*More Data*" (bit 13), é utilizado para comunicar a uma STA que esteja em modo "*power-save*" e que para além da trama corrente existem mais tramas pendentes em *buffer* que lhe estão destinadas. Depois da recepção de uma trama com este campo a "1" a estação receptora pode escolher manter-se à escuta mais algum tempo para receber as tramas que lhe estão destinadas e estão em espera (*queue*) para envio, ou por forma a economizar energia mantém-se no estado "*power-save*" e o AP deverá manter em "*buffer*" as tramas até que a estação transite para modo normal no próximo ciclo.
- O campo "*Prot. Frm.*" (i.e., *Protected Frame*) (bit 14) é utilizado para indicar que a trama está protegida por um dos mecanismos de cifra suportados no IEEE 802.11. Este campo designava-se por WEP (*Wired-equivalent Privacy*) na norma original IEEE

802.11 de 1999, mas o *Taskgroup* IEEE 802.11i TG alterou o seu nome para *Protected Frame*.

- O campo "*Order*" (bit 15), quando a “1” indica que um MSDU está a ser transmitido usando a classe de serviço "*strictly ordered*" disponibilizada pelo 802.11 MAC. Nestas condições não poderá ser enviado qualquer outro MSDU até que o corrente seja transmitido completamente. Uma STA não pode receber tráfico usando a classe de serviço "*strictly ordered*" se já optou pela utilização de gestão de energia (*power management*).

4.5.3. Tramas de controlo do IEEE 802.11

Todas as tramas de controlo (Figura 4-24) têm uma dimensão reduzida e têm como objectivo controlar o acesso ao meio, indicando aos dispositivos quando devem iniciar ou terminar a transmissão e quando há situações de erros na transmissão.

Dos seis tipos de tramas definidos, as primeiras quatro (*Request-to-Send, Clear-to-Send, Acknowledgment,* e *Power-Save Poll*) são utilizadas no protocolo de controlo de acesso ao meio *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) no método de acesso *Distributed Coordination Function* (DCF) enquanto os dois tipos de tramas (*CF-End e CF-End+CF-ACK*) restante são utilizadas no método de acesso opcional *Point Coordination Function* (PCF).

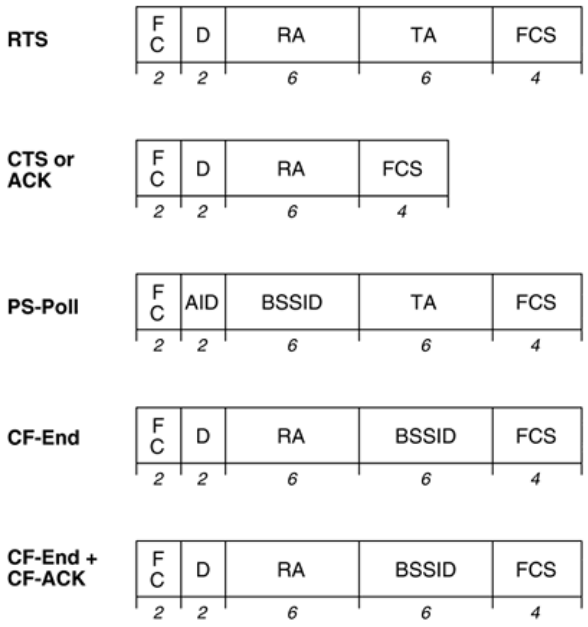

Figura 4-24: Tramas de Controlo IEEE 802.11.

4.5.3.1. Tramas de controlo RTS e CTS do IEEE 802.11

O mecanismo de RTS/CTS pode ser utilizado para proteger a transmissão de um MPDU ou MMPDU, através da reserva do meio de transmissão antes da transmissão da trama. Este mecanismo é utilizado por cada trama a transmitir entre a STA emissora e o AP, podendo o AP optar pela utilização ou não do mecanismo RTS/CTS na transmissão para a STA receptora. O conceito de protecção significa a reserva do meio de transmissão por um determinado intervalo de tempo suficiente para transmitir uma trama e receber a trama de controlo *Acknowledgment* (ACK). A reserva do meio apenas se aplica a dispositivos (STA) que ouçam a troca de tramas RTS/CTS, sendo possível a existência de STA que fiquem num determinado instante ao alcance do meio previamente reservado e que, encontrando o meio livre (*idle*), comecem uma transmissão causando interferências no meio.

Este mecanismo permite o funcionamento num ambiente que na literatura se designa por *Hidden Station* e que será descrito quando da descrição do método *Distributed Coordination Function* (DCF).

A trama *Request-to-Send* (RTS) tem um tamanho de 20 bytes e é utilizada opcionalmente como forma de reservar o meio durante um intervalo de tempo. Depois de ter sido recebida a correspondente trama de resposta *Clear-to-Send* (CTS) a STA pode enviar a sua trama de dados

ou gestão, visto que todas as tramas que estão a funcionar num modo de funcionamento BSS escutaram o CTS enviado pelo AP.
Em cada dispositivo por onde a trama passa é decidido de forma independente pela utilização do mecanismo RTS/CTS para a próxima transmissão. Uma STA ou um AP tem um parâmetro na configuração chamado *RTS Threshold* que determina se uma trama é precedida por uma troca de tramas RTS/CTS. Tramas de tamanho inferior ao definido no *RTS Threshold* ou tramas de *multicast* nunca são precedidas da troca de tramas RTS/CTS.

4.5.3.2. Tramas de controlo ACK do IEEE 802.11

As tramas de controlo de *Acknowledgment* (ACK) são utilizadas para indicar que a recepção de uma trama foi efectuada com sucesso. Se o emissor não receber um ACK durante uma janela temporal expectável depois de transmitir uma trama, irá reenviar a trama numa próxima oportunidade. A utilização do ACK no IEEE 802.11 serve actualmente para indicar ao emissor quando ocorreu uma colisão (aferida pela falta de um ACK).

4.5.3.3. Tramas de controlo PS-Poll do IEEE 802.11

A trama de controlo PS-Poll (*Power-Save Poll*) é usada por um dispositivo STA quando verifica que um AP tem tramas em *buffer* que lhe são destinadas. Este mecanismo é utilizado quando uma STA sai de um modo "*power-save*" e necessita de receber as tramas guardadas entretanto pelo AP.

4.5.3.4. Tramas de controlo CF-End e CF-End+CF-ACK - IEEE 802.11

Estas duas tramas de controlo CF-End (*Contention-Free-End*) e CF-End+CF-ACK (*Contention-Free-End Acknowledgment*) são utilizadas no método de acesso opcional *Point Coordination Function* (PCF). Ambas são enviadas com endereço destino de *broadcast* e ambas têm o campo "*Duration*" com valor 0.

4.5.3.5. Tramas de gestão do IEEE 802.11 (MMPDUs)

Existem mensagens que a STA e o AP utilizam para negociar e controlar a sua relação que estão definidas na norma IEEE 802.11 através dos seguintes tipos de mensagens de gestão:

- Beacon (notificação)
- Probe (Request e Response)
- Authentication (Request e Response)
- Association (Request e response)
- Reassociation (Request e Response)
- Disassociation (notificação)
- Deauthentication (notificação)
- IBSS Announcement Traffic Indication Message (ATIM) (notificação)

Os tipos de tramas indicados como "notificação" caracterizam-se pelo facto de, ao ser enviada uma trama desse tipo, não se esperar nenhuma resposta.

O corpo de uma mensagem de gestão está dividido em duas partes (Figura 4-25). A primeira corresponde a um conjunto de campos fixos específicos de cada mensagem de gestão e a segunda parte contém elementos de número variável relevantes para o dispositivo receptor.

A utilização de elementos de número variável traz vários benefícios:

- A utilização de elementos permite que a norma seja actualizada mais facilmente. Por exemplo, a informação necessária para um novo método de segurança pode ser colocada nestes campos, tendo como vantagem que dispositivos mais antigos que não entendam estes novos elementos podem ignorá-los.
- Alguns fabricantes podem implementar funções especiais. Por exemplo a inclusão de informação proprietária nas tramas "*beacons*" que indicam para os dispositivos do mesmo fabricante a taxa de ocupação dos AP.

Cada elemento é caracterizado por ter um formato similar com três componentes. O primeiro byte representa o "*Type"*, o segundo byte representa o tamanho em bytes do elemento e a terceira componente representa a informação do elemento.

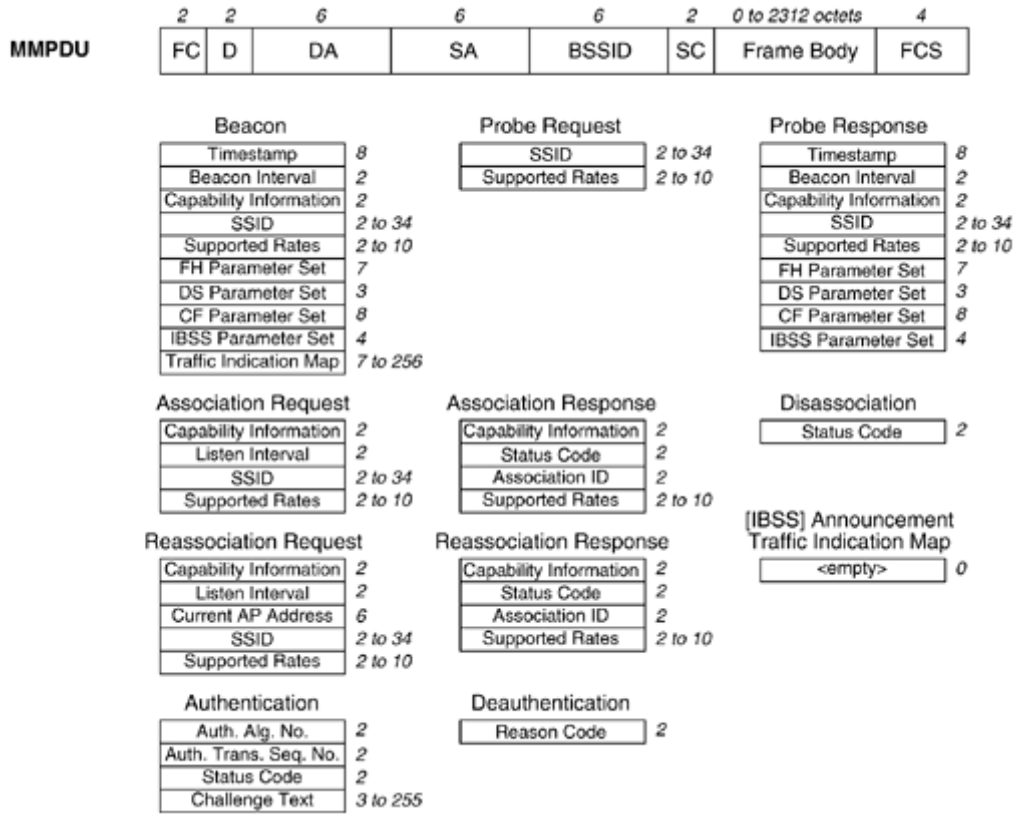

Figura 4-25: Tramas de gestão do IEEE 802.11.

4.5.3.6. Funcionamento básico no modo infra-estrutura

Uma estação que se queira ligar a uma rede sem fios deve primeiro verificar se a WLAN está presente. Este processo (Figura 4-26) pode ser feito de uma forma passiva (escutando uma trama de gestão -*Beacon*, enviada pelo AP) ou de uma forma activa (através do envio de trama de gestão *Probe Request* em todos os canais disponíveis, até que receba uma trama *Probe Response* proveniente de um AP.

Se a STA verifica que a WLAN está presente e que se quer juntar à mesma, passa para a fase de autenticação através do envio de uma mensagem *Authentication Request*. A resposta do AP é feita através da mensagem *Authentication Response*. Uma estação poderá estar autenticada em vários AP antes de se associar ao AP através do qual irá transmitir a suas tramas de dados.
Estando uma STA autenticada num AP poderá esta estabelecer uma ligação através da mensagem *Association Request*, ao qual o AP responderá com *Association Response* confirmando ou não o estabelecimento da ligação.

Estando uma STA autenticada e associada a um AP pode enviar dados para o AP, que depois os reencaminhará para uma LAN ou para outra STA.

A Figura 4-26 mostra os estados em que se podem encontrar as STA e quais as tramas permitidas em cada estado.

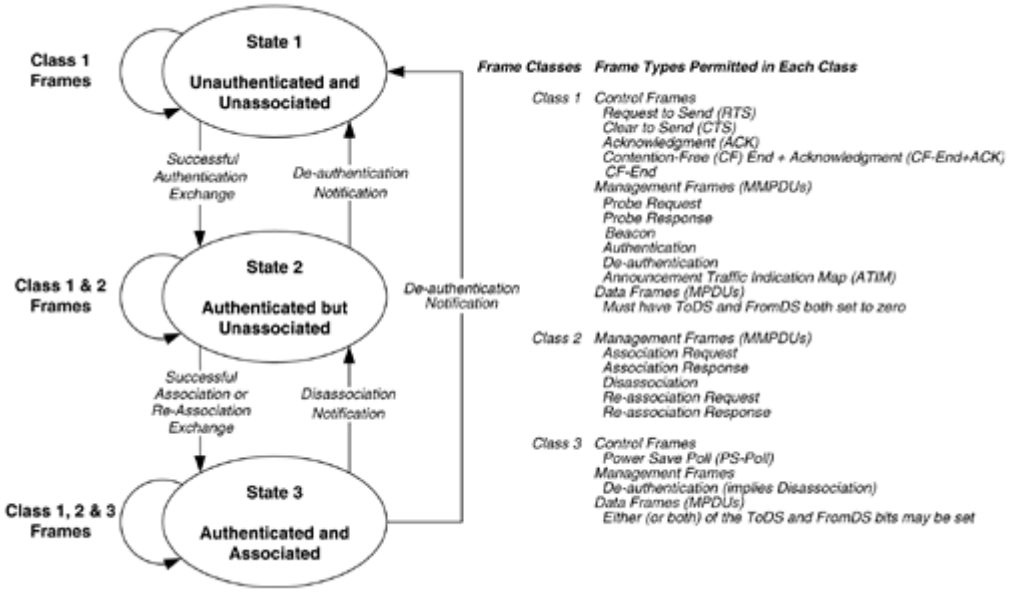

Figura 4-26: Máquina de estados de autenticação e associação

Como a fase de autenticação precede a fase de associação é possível a uma STA autenticar-se em vários AP, apesar de apenas poder estar associado a um AP. Esta funcionalidade permite a movimentação (*roaming*) da STA de um AP para outro AP através da desassociação num AP (*Disassociation Request*) e de uma associação noutro AP (*Reassociation Request*). A STA pode usar parâmetros como seja a potência do sinal ou a qualidade do sinal para optar em qual AP se quer associar.

4.5.3.7. Tramas Beacon

Tal como já foi referido o envio de tramas "*beacon*" é o método pelo qual um AP anuncia a sua presença e mantêm uma base de sincronia temporal na rede. Estas tramas são enviadas regularmente pelo AP (Figura 4-27), tipicamente de 100 em 100 *ms* e contêm informação útil como seja o nome da rede e taxas de transmissão suportadas pelo AP. Depois do processo de associação da STA ao AP estas tramas servem para informar que o AP se mantém em

funcionamento e que se mantém com cobertura de sinal possibilitando também alguns modos de funcionamento como sejam o "*power save*".

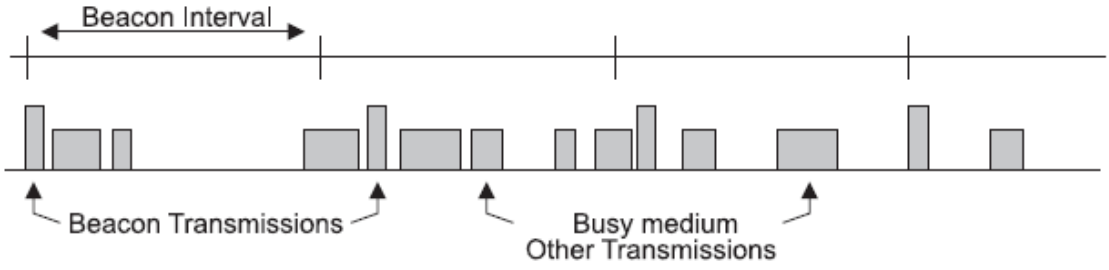

Figura 4-27: Transmissão de tramas Beacon num meio com elevada ocupação

A estrutura desta trama contempla 10 campos dos quais só os primeiros 3 são obrigatórios.

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set information element is present within Beacon frames generated by STAs using frequency-hopping PHYs.
7	DS Parameter Set	The DS Parameter Set information element is present within Beacon frames generated by STAs using direct sequence PHYs.
8	CF Parameter Set	The CF Parameter Set information element is only present within Beacon frames generated by APs supporting a PCF.
9	IBSS Parameter Set	The IBSS Parameter Set information element is only present within Beacon frames generated by STAs in an IBSS.
10	TIM	The TIM information element is only present within Beacon frames generated by APs.

Figura 4-28: Campos das tramas Beacon

- *Timestamp*

Este campo é inicializado quando o AP inicia o seu funcionamento e continua sempre a crescer em unidades de milissegundos. Este campo tem 64 bits, pelo que demoraria cerca de meio milhão de anos a atingir o limite. O valor deste campo é utilizado para sincronia temporal pelos dispositivos associados.

- *Beacon Interval*

Este campo informa quando é que o próximo Beacon é esperado. O valor por defeito para este campo é de 100 milissegundos.

- *Capability Information*

Este campo identifica quais as funcionalidades opcionais que o AP suporta.

- SSID

O SSID (ou nome de rede) é um campo opcional e apresenta a identidade da rede que o AP suporta.

- *Supported Data Rates*

Este campo é opcional e informa quais as velocidades de transmissão que o AP suporta. O exemplo apresentado na Figura 4-29 mostra o suporte a 4 velocidades de transmissão.

- Parâmetros associados à transmissão rádio.

Existem diversos parâmetros opcionais que são mutuamente exclusivos. Se existir o FH (*Frequency Hopping*) então o parâmetro DS (*Direct Sequence*) não poderá estar presente (e vice-versa). O parâmetro CF (*Contention Free*) aparece em tramas *Beacon* ou *Probe Responses* provenientes de um AP onde o modo *Point Coordinator* está em funcionamento. O parâmetro IBSS é enviado pelas estações quando estão a funcionar no modelo de IBSS (onde não existem APs).

- TIM (*Traffic Indication Map*)

Este campo é utilizado para informar os dispositivos que estão no modo *power-save* que existem dados pendentes no AP. Os dispositivos no modo *power-save* apenas ficam activos para a recepção das tramas *beacon* por forma a permitir a redução dos gastos de energia quando não existe informação para transmitir ou receber.

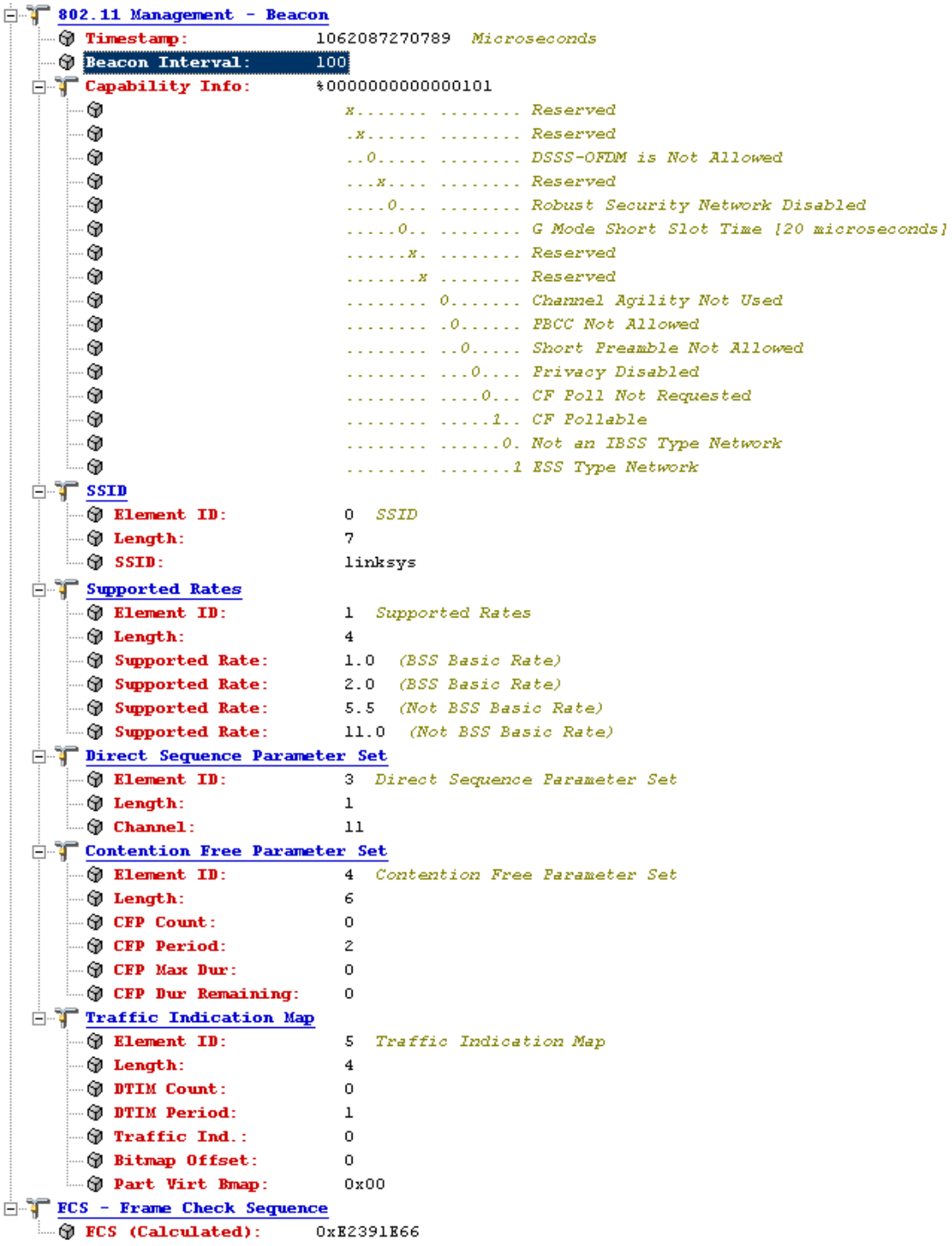

Figura 4-29: Exemplo de uma trama *Beacon*

4.5.3.8. Tramas *Probe*

Uma estação que queira juntar-se a uma rede sem fios deve verificar se a WLAN está presente. Este processo pode ser efectuado de forma passiva (através da escuta da tramas *Beacon*

enviadas pelos AP) ou de forma activa (através do envio de uma trama "*Probe Request*" em todos os canais disponíveis até que o AP responda através de uma trama "*Probe Response*").

A desvantagem de utilizar um processo de procura (*scan*) passivo é o facto de uma STA não conhecer à *priori* qual o canal que está a ser utilizado, pelo que deve escutar cada canal durante certo intervalo de tempo antes de ir comutar a pesquisa para outro canal. É possível que este processo leve muito tempo até que a STA consiga receber uma trama *Beacon* e logo identifique os parâmetros de transmissão correctos.
Alternativamente a utilização de um processo de pesquisa activo permite à STA controlar o envio das tramas *Probe Request* em cada canal e desde que espere o tempo suficiente para escutar uma trama *Probe Response* terá uma garantia da existência ou não de um AP no canal sendo desta forma mais rápido o processo de detecção da rede.
A trama *Probe Response* tem os mesmos campos da trama *Beacon* com excepção da ausência do campo TIM (uma vez que o AP não deverá ter dados para enviar para uma STA que não estará num estado autenticado).

Os tempos de detecção de um novo AP são importantes e têm reflexos em aplicações (que estejam em estações em movimento e que necessitem de transitar de AP), nas vertentes de desempenho, garantia de serviço e de segurança.

4.5.4. Tramas de dados do IEEE 802.11 (MPDUs)

Todas as normas do IEEE 802.11, independente da banda de frequência em que funcionem usam o formato de trama apresentado na Figura 4-30 e é designado oficialmente por *MAC Protocol Data Unit* (MPDU). Os campos *Address4* e *QoS Control* são opcionais e dependes do conteúdo do campo FC.

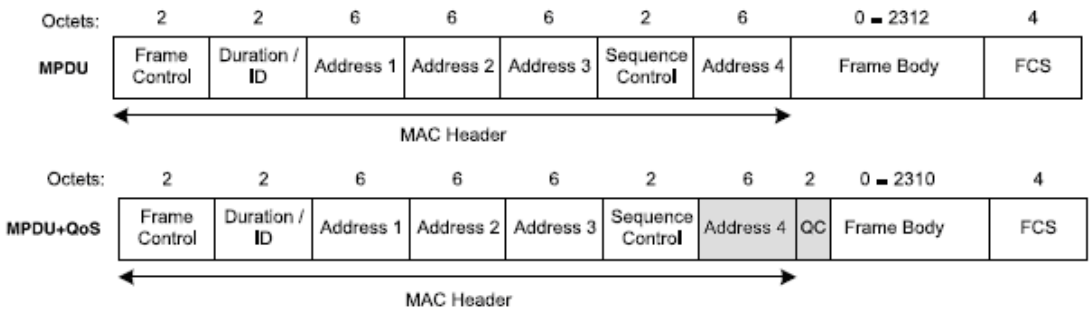

Figura 4-30: Estrutura de uma trama de Dados IEEE 802.11

O tamanho máximo de um MPDU é de 2346 bytes. Destes, estão reservados 24 ou 30 bytes para o *header* MAC e 4 bytes para o FCS, ficando disponíveis 2310 ou 2316 (sem entrar em consideração com o campo QC referenciado no IEEE 802.11e.

4.6. Protocolo de acesso ao meio

As funções principais do nível MAC são a coordenação e controlo do acesso e partilha do meio pelas estações e definir a relação entre as tramas a transmitir e o sinal de nível físico. Existem diversos métodos de funcionamento para acesso ao meio descritos no mecanismo *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA).

4.6.1. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Uma das grandes diferenças entre a Ethernet e o 802.11 WLAN é a forma como é controlado o acesso ao meio, determinando quem e quando pode comunicar. A Ethernet utiliza o mecanismo CSMA/CD onde uma estação pode enviar e escutar o meio em simultâneo detectando colisões se houver diferenças nos dados transmitidos e enviados. No entanto quando se transmite em ondas de rádio e se tenta escutar o meio em simultâneo, a sua própria transmissão "abafa" todas as outras, impossibilitando a detecção de colisões. Existe uma outra grande diferença entre as tecnologias e que consiste no facto de todas as estações num segmento Ethernet se ouvirem entre si enquanto numa rede sem fios nem sempre poderá ser possível. Por estas razões utiliza-se o mecanismo de *Collision Avoidance* - Figura 4-31 - que está definido ao nível MAC através dos métodos de acesso *Distributed Coordination Function* (DCF) e *Optional Point Coordination Function* (PCF).

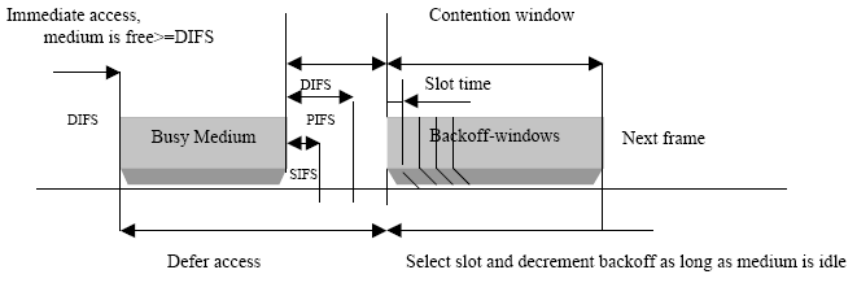

Figura 4-31: Mecanismo Collision Avoidance.

4.6.2. Necessidade de ACK positivo

A norma IEEE 802.11 define um esquema para proporcionar fiabilidade na transmissão sem fios. Todas as tramas *unicast* devem ter uma trama ACK em resposta. Quando uma estação recebe uma trama de dados deve responder com uma trama de ACK ao emissor, de forma que este saiba que a trama de dados foi bem entregue. Se por qualquer razão o emissor não receber a trama de ACK irá assumir que a trama de dados não foi entregue e irá retransmiti-la. Existe um valor máximo de retransmissões a partir do qual a trama é descartada.

A desvantagem do mecanismo de ACK é o *overhead* que adiciona à comunicação e a correspondente perca na taxa de transmissão, bem como o aumento dos intervalos de espera (*delay*). No entanto este mecanismo é necessário para permitir o bom funcionamento das redes sem fios.

4.6.3. Espaçamentos temporais *interframe*

O IEEE 802.11 define quatro espaçamentos temporais - Figura 4-32 - utilizados nas regras de acesso ao meio para priorizar a transmissão de certas tramas. Estes espaçamentos têm uma base temporal dependendo do meio físico e estão relacionados algebricamente entre si. Os temporizadores são utilizados no processo de contenção de acesso ao meio, para garantir operações atómicas como seja o mecanismo RTS/CTS.

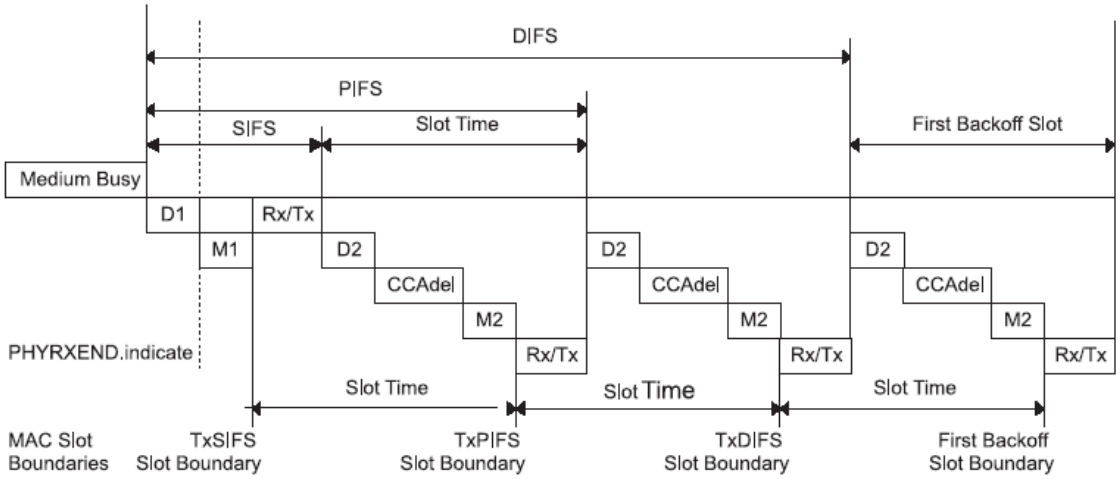

Figura 4-32: Relação temporal entre SIFS,PIFS e DIFS.

- SIFS (*Short Interframe Space*)

O SIFS é utilizado para priorizar tramas que são enviadas imediatamente a um RTS (*Request to Send*) como sejam ACK ou CTS (*Clear to Send*).

- PIFS (*PCF Interframe Space*)

O PIFS é utilizado para dar prioridade a tramas que utilizem o mecanismo de gestão de contenção PCF (*Contention Free*).

- DIFS (*DCF Interframe Space)*

O DIFS é o tempo mínimo que o meio deve estar livre antes de qualquer transmissão baseada no processo de contenção DCF.

- EIFS (*Extended InterFrame Space*)

O EIFS é um intervalo de tempo variável que é utilizado quando uma trama é recebida com erros.

4.6.4. Optional Point Coordination Function (PCF)

Este método é opcional e é utilizado normalmente para implementação de serviço dependentes do tempo como transmissão de Voz e Vídeo. Consiste em colocar um coordenador (um AP) a controlar o acesso ao meio. O AP divide temporalmente o acesso entre o modo PCF e DCF. Enquanto está a funcionar em modo PCF o AP pergunta/pede (através de *poll*) por dados a cada estação a intervalos de tempo definidos possibilitando a garantia de um valor de latência máximo. Consegue-se assim atrasos de transmissão baixos e evitar colisões visto que as estações só podem transmitir quando são autorizadas.

4.6.5. Distributed Coordination Function (DCF)

Neste método as estações devem analisar o meio para verificar se está ocupado com outra transmissão ou se está livre para iniciar a transmissão. Por forma a ser resolvido a contenção entre as várias estações que aguardam pela libertação do meio, o CSMA/CA define algoritmo "*exponential backoff*" que funciona da seguinte forma:

- De cada vez que uma estação tenta transmitir, verifica se o meio está livre durante o intervalo DIFS (ou EIFS no caso de uma recepção incorrecta). De seguida a estação espera um intervalo chamado de "*contention window*" dividido em intervalos de tempo dependentes do meio físico. A escolha do número de intervalos de tempo (*Backoff Time*) é aleatória e corresponde ao tempo que a estação espera para iniciar a transmissão. A estação com menor número de intervalos é a que inicia a transmissão.

- Com a ocupação do canal de transmissão pela estação ganhadora, as outras estações suspendem o processo de espera de espera (*backoff*) até que o meio esteja livre de novo. As estações que suspenderam o processo de espera, logo que o meio fique livre deverão continuar a decrementar o número de intervalos (*BackoffTime*) por forma a poderem ter uma maior probabilidade de obter o meio.
- O número aleatório de intervalos (*Backoff Time*) é escolhido no intervalo [0,CW], sendo CW o tamanho da "*Contention Windows*". Este mecanismo é chamado de "*exponential backoff*" porque depois de uma transmissão falhada a estação deverá duplicar o valor da CW de forma a reduzir a probabilidade de colisões em rede com muita carga. O valor de CW pode assumir valores entre *aCWmin* e *aCWmax*, tendo em atenção que o valor de CW não irá aumentar ao ser atingido o máximo – Figura 4-33.
- As colisões que ocorram entre duas estações que tenham seleccionado o mesmo número de *slots* só são detectadas pela falta da trama ACK correspondente à transmissão, uma vez que uma estação não consegue escutar o meio durante a transmissão.

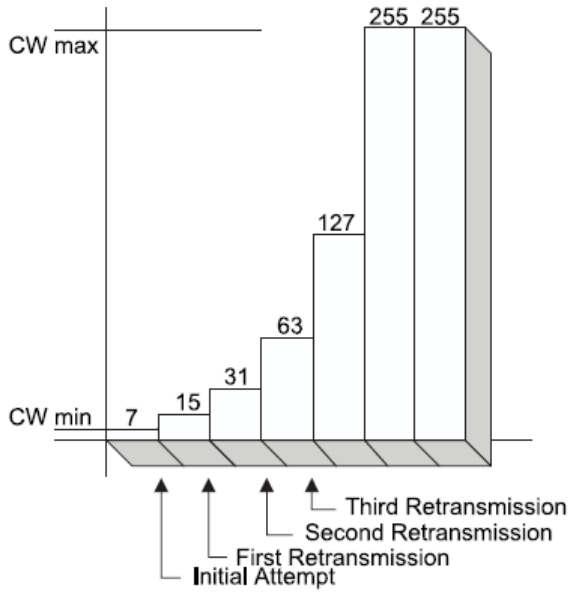

Figura 4-33: Exemplo do incremento exponencial do CW

O meio *Wireless* possibilita uma situação (*Hidden Station*) onde duas estações não se "ouvem" mas conseguem ambas falar com um AP - Figura 4-34.

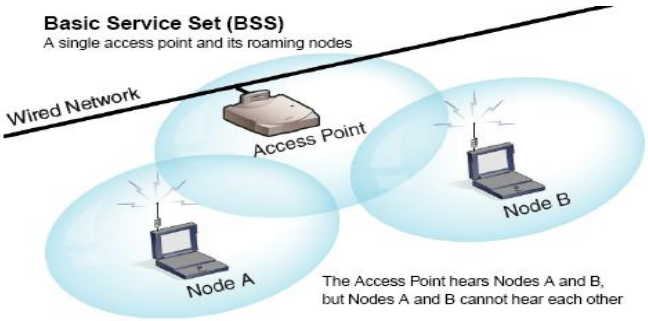

Figura 4-34: Problema da estação invisível.

Esta situação possibilita que ambas as estações avaliem o meio e transmitam em simultâneo provocando colisões no meio impossibilitando o AP de receber os dados. Para reduzir a probabilidade de colisões foi criado um mecanismo de protecção na norma chamado *Virtual Carrier Sense*.

4.6.6. Virtual Carrier Sense

O método de detecção de ocupação do meio pode ser físico ou virtual. A detecção física é obtida pelo nível físico. A detecção virtual é efectuada através da utilização do *Network Allocation Vector* tal como mostrado na Figura 4-35.

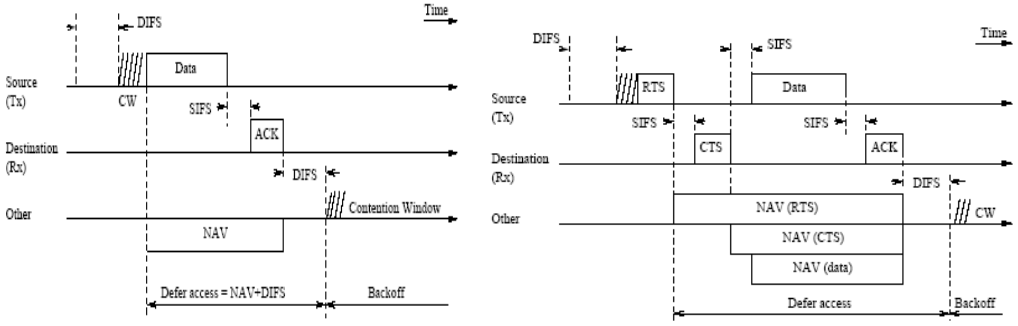

Figura 4-35: DCF CSMA/CA e funcionamento RTS/CTS.

Uma estação que necessite de transmitir dados envia primeiro um pacote de controlo pequeno chamado *Request-to-Send* (RTS) onde inclui dados da origem, destino e duração da transacção. Se o meio está livre o AP responde com um pacote de controlo pequeno chamado *Clear-To-Send* (CTS) com a mesma informação de duração. Todas as estações que recebem o RTS ou o CTS colocam o seu indicador *Network Allocation Vector* (NAV) e não tentam efectuar transmissões durante o período de duração recebido. Este método reduz a probabilidade de colisões nos receptores mesmo em estação "invisíveis" a estações emissoras visto que, os receptores ouvem o RTS e reservam o meio como ocupado durante a duração especificada no RTS. No fim da transmissão o AP ou a estação receptora envia um ACK. No entanto o

cabeçalho do MPDU é observável por todas as STAs, garantindo assim o funcionamento do protocolo. O campo *Duration/Identification* é utilizado pela estação emissora para indicar a quantidade de tempo que prevê utilizar o meio, incluindo o tempos de transmissão e o correspondente ACK, de forma a que as outras estações possam actualizar o seu NAV e manter-se "silenciosas" até que o processo de trama/ACK esteja terminado.

5. Segurança em redes 802.11

5.1. Introdução

A tecnologia de redes sem fios baseada na norma IEEE 802.11 trouxe grandes benéficos aos utilizadores em casa, nas empresas ou em locais públicos. Oferecendo um método de ligação a redes rápidas sem necessidade de fios proporcionou mobilidade e produtividade, mas trouxe novos desafios na implementação de mecanismos de segurança, não existentes nas redes com fios.

\(Wireless) baseadas em tecnologia de rádio frequência (RF) expõem a informação no meio rádio até ao alcance das ondas de rádio sem barreiras físicas.

A norma de segurança inicialmente introduzida no IEEE 802.11 de 1997 não foi alterada na rectificação da norma de 1999 e consiste na implementação do protocolo *Wired Equivalent Privacy* (WEP). O WEP foi desenhado para ser um protocolo simples, que poderia ser implementado em *software* ou *firmware* a baixo custo e encontra-se implementado em todos os AP e drivers de mercado. Ao longo dos primeiros anos foram-se descobrindo diversas falhas no WEP, facilmente utilizáveis por qualquer um através de diversas ferramentas [5] presentes na Internet. Em resposta o *IEEE Task Group I* desenvolveu e apresentou em 2004 uma nova norma de segurança conhecida como *Robust Security Network* (RSN) que responde todos os ataques e vulnerabilidades conhecidos melhorando significativamente a segurança nas componentes de autenticação e privacidade.

Para impedir o acesso não autorizado a uma rede WLAN, uma solução de segurança robusta deve proporcionar mecanismos fortes de autenticação e privacidade. Autenticação refere-se ao processo pelo qual a identidade de um dispositivo é verificada antes que a ligação à rede esteja concluída. A autenticação mútua deverá ser utilizada para a verificação das identidades dos dois interlocutores da ligação. Neste caso a identificação de um dispositivo (estação cliente) à rede é verificada pela rede e a identificação da rede é verificada pelo dispositivo cliente.

Depois da autenticação mútua, a ligação entre a estação e a rede é estabelecida e os mecanismos de privacidade são utilizados para proteger os dados que são enviados na ligação da rede sem fios.

A privacidade envolve a cifra dos dados impedindo o acesso por quem quer que escute o meio e que não esteja autorizado. Um bom mecanismo de privacidade também inclui mecanismos de protecção que assegurem que os dados não são alterados em trânsito até ao destino e que valida os endereços do emissor e do receptor dos dados.

5.2. Segurança no IEEE 802.11

O que significa segurança? Quando esta palavra é utilizada no contexto de redes de computadores refere-se tipicamente a um número de serviços entre os quais a autenticação (de utilizadores e de dados), autorização (controlo de acesso) e cifra (para garantir confidencialidade ou para proteger dados de serem vistos por terceiras partes).

No contexto das WLANs, a segurança aplica-se ao nível do controlo de acesso (permitindo que os utilizadores válidos se juntem à WLAN), da autenticação mútua (a STA pode assegurar-se que está a falar com um AP legitimo e vice-versa), e cifra (o tráfego que atravessa o ar é ilegível para quem escute). A cifra é activada através de mecanismos de distribuição de chaves; idealmente as chaves são escolhidas aleatoriamente, trocadas de forma segura e utilizadas apenas uma única vez.

Dentro do alcance de um receptor, uma STA no ambiente WLAN pode ouvir tudo o que é transmitido por qualquer outra STA. A trama pode estar cifrada, o que converte a parte de dados da trama num conteúdo aleatório semelhante a "ruído" de comunicações e que apenas tem sentido e é percebido por quem possui a necessária chave de cifra de decifra (*decryption*).

Tal como já referido a segurança da rede compreende alguns serviços (3.1.1), autenticação de utilizadores, autenticação de mensagens, integridade e confidencialidade, podendo ser utilizadas separadamente ou em conjunto.

A autenticação é um termo que tem pelo menos dois significados:

Um dos significados, associado aos protocolos de rede, envolve a utilização de técnicas de criptografia para assinar as mensagens, de tal forma que há garantia que apenas um determinado emissor a poderia ter enviado, com aplicação a sistemas que apenas necessitam de garantir que as mensagens não foram alteradas em trânsito e não sendo importante manter confidencial o conteúdo das mensagens. O serviço de autenticação de mensagens pode ser utilizado para

proporcionar serviços de não-repudiação, garantindo a todos os receptores da mensagem que esta apenas poderia ter sido emitida por um emissor específico (utilizando uma chave privada). Em termos práticos a não repudiação só será efectiva se o emissor conseguir "guardar" a sua chave privada de uma forma segura.

Os protocolos (3.5, 3.6) que proporcionam autenticação de mensagens utilizam em princípio funções de síntese (*hash*) de um só sentido. O resultado destas funções é chamado de *Integrity Check Value* (ICV), *Message Integrity Code* (MIC) ou *Message Authentication Code* (MAC), dependendo do contexto. Os parâmetros de entrada para estas funções consistem tipicamente nos dados a proteger e a chave de cifra (ou um numero derivado da chave no caso do MAC (3.6.1)). Sem a utilização da função de síntese (*hash*) com uma chave de cifra, qualquer um poderia copiar uma trama válida, alterar os dados, recalcular o valor de *hash* que faz correspondência com os novos dados, fazendo com que o receptor aceitasse a trama como válida.

Um outro aspecto da autenticação é utilizado para determinar como e quando os utilizadores podem aceder à rede e aos seus recursos. Através de um conjunto de protocolos e serviços conhecidos colectivamente como *Authentication, Authorization, and Accounting* (AAA), os utilizadores autorizados podem aceder à rede e seus recursos. A função do AAA foi considerada importante para que o IETF criasse um *Working Group* (WG) para criar normalização relacionada com estes aspectos de segurança.

Os protocolos mais frequentemente associados a serviços AAA são o *Remote Access Dial-In User Service* (RADIUS; RFC-2865) [34] e o *Diameter* (RFC-6733) [35], havendo também outros protocolos que poderão ser utilizados para estas funções como sejam *Common Open Policy Service* (COPS; RFC-4261 [36]) e o *Simple Network Management Protocol* (SNMPv3; STD-62; RFC 5343, RFC 5590).

Existem alguns protocolos proprietários ainda em uso entre os quais o *Terminal Access Controller Access Control System* (TACACS) e o TACACS+, especificados pela Cisco e suportados por muitos fabricantes no acesso a aplicações em modo terminal a *Terminal Servers* ou a *Routers*.

Finalmente o serviço de confidencialidade é normalmente disponibilizado através da utilização de algoritmos criptográficos para cifrar os dados, utilizando chaves secretas (também chamados

algoritmos simétricos (3.4.3)) ou chaves públicas (também designados por algoritmos assimétricos (3.4.4)). Em ambos os algoritmos o conhecimento de chaves é que permite a comunicação entre interlocutores, sendo que no primeiro a chave secreta é igual tanto para as operações de cifra como de decifra. Nos algoritmos assimétricos cada interlocutor tem uma chave privada e uma chave pública, sendo disponibilizada a chave pública a quem queira comunicar com determinado interlocutor.

Existem diversos tipos de algoritmos de chaves secretas, subdivididos em cifras contínuas (*stream-oriented)* e cifra por blocos (*block-oriented*) (3.4.1). O melhor exemplo de uma cifra continua é o algoritmo RC4 utilizado no WEP enquanto para algoritmos de cifra por blocos existem o *Data Encryption Standard* (DES), *Triple-DES* e o *Advanced Encryption Standard* (AES). Os algoritmos de cifra têm estado presentes ao longo do desenvolvimento dos protocolos de segurança nas redes sem fios (Figura 5-1).

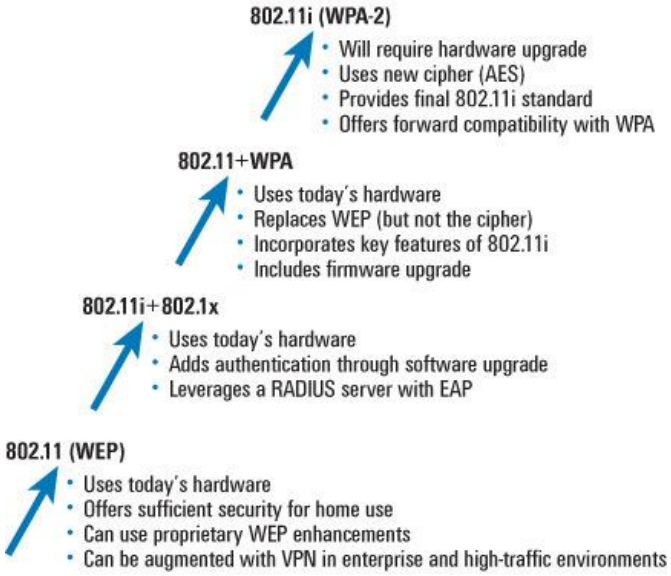

Figura 5-1: Evolução dos protocolos de segurança

5.3. Serviços de autenticação

A norma IEEE 802.11 define dois modos de validar utilizadores que tentam obter acesso à rede: *Open-system* e Shared-key (Figura 5-2). A técnica de autenticação *Open-system* não é na verdade uma autenticação uma vez que o AP aceita o acesso do dispositivo móvel sem verificar a sua identidade. A autenticação *shared-key* é baseada na utilização de técnicas criptográficas para possibilitar o acesso do dispositivo móvel ao AP.

Antes que um dispositivo (STA) se possa ligar a uma rede, terá que se identificar. O nível de com que se confia depende da configuração no dispositivo (STA) e das credenciais do utilizador. Nas redes WLANs iniciais (baseadas na norma IEEE 802.11-1999), uma estação deveria inicialmente "autenticar-se" com um AP ao seu alcance rádio necessitando de um de dois tipos de trocas de pacotes.

Quando utilizamos cifra para criar uma ligação, os dois lados formam uma "associação de segurança", que corresponde ao nome formal para o conjunto de características que definem a relação entre a STA e o AP (em modo infra-estrutura) ou entre duas STA (em modo IBSS). Uma associação de segurança pode conter algumas (ou todas) das características seguintes envolvidas na ligação: o protocolo de gestão de chaves de autenticação (se existir), grupos de cifra (*cipher suits*) para *unicast* e *multicast*, chaves criptográficas, tempo de vida das chaves e outros paramentos relacionados com o funcionamento dos sistemas criptográficos.
O primeiro passo para definir uma associação de segurança é executar uma autenticação para garantir que cada uma das partes encontra e aceita a outra através dos métodos que achar necessário verificar.

Existem três "estados" onde uma STA se pode encontrar relativamente a um AP (Figura 4-26).
No primeiro estado uma STA encontra-se numa situação de não autenticada e não associada. Neste estado, a STA apenas pode enviar tramas de gestão para poder estabelecer uma autenticação. É também possível enviar algumas tramas de controlo que são necessárias para participar no protocolo MAC, como sejam as tramas *Request to Send* (RTS) e Clear to Send (CTS). Só quando a STA está em modo IBSS, é possível enviar tramas de dados neste estado. Se uma estação se autenticou com sucesso poderá passar para o segundo estado.

O segundo estado é caracterizado por uma situação onde a STA está autorizada mas não se encontra associada a um AP. Neste estado a STA poderá enviar mais tipos de tramas, especificamente MMPDUs, relativas a processo de Associação, Re-Associação e Desassociação. Recordemos que uma STA poderá estar associada apenas a um AP de cada vez, apesar de poder estar autenticada em vários. Após ter efectuado o processo de associação com sucesso passa para um terceiro estado.

O terceiro estado é atingido quando um STA se associa a um AP. Neste estado as tramas de dados podem ser enviadas através do AP e a STA pode aceder às redes com fios onde o AP se encontra ligado (*Distribution System Service – DSS*).

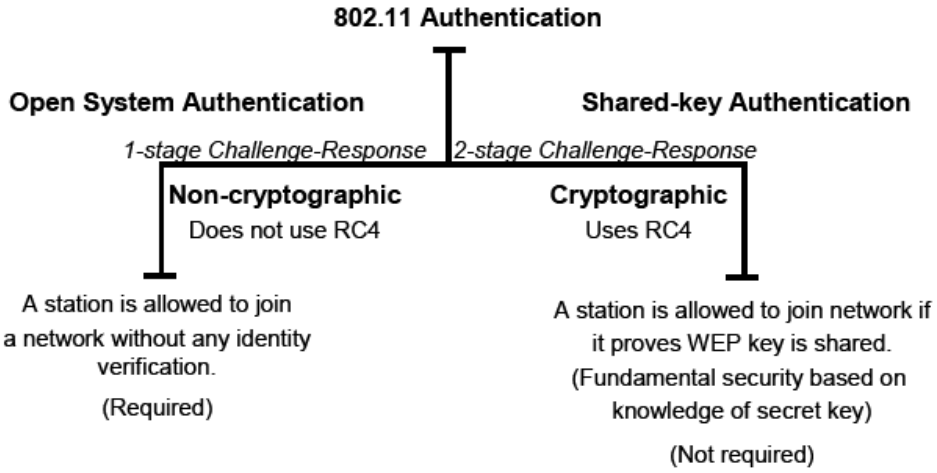

Figura 5-2: Taxonomia das técnicas de autenticação IEEE 802.11.

5.3.1. Autenticação "*Open System*"

O termo autenticação "*Open System*" é semanticamente equivalente a "Não tem autenticação". Numa autenticação *Open System*, a WLAN está aberta a qualquer potencial utilizador, que necessita apenas de efectuar uma troca de mensagens básicas de autenticação, que apenas tem como objectivo a identificação do seu endereço MAC por parte do AP. No caso de se estar a trabalhar no modo IBSS, esta forma de autenticação de utilizador pode ser utilizada entre duas STAs, apesar de não ser obrigatória a autenticação ao nível MAC.

Segundo a norma IEEE 802.11-1999 as trocas de mensagens de autenticação utilizam tramas de gestão *Management MAC Protocol Data Unit* (MMPDU). O campo *Frame Control* da MMPDU é mostrado na Figura 5-3. As tramas MMPDU utilizadas para negociar a autenticação têm o "*Type"* = "00" (gestão) e o "*Sub-Type*" com "1100" (autenticação) ou "0011" (desautenticação).

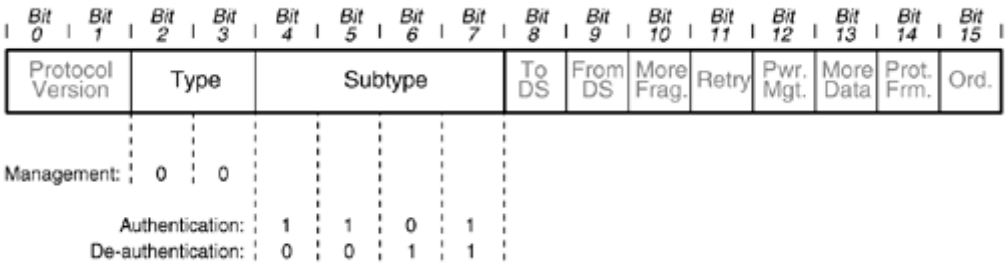

Figura 5-3: Campo *Frame Control* de um MMPDU no processo de autenticação.

A autenticação *Open System* consiste apenas em duas mensagens como mostrado na Figura 5-4.

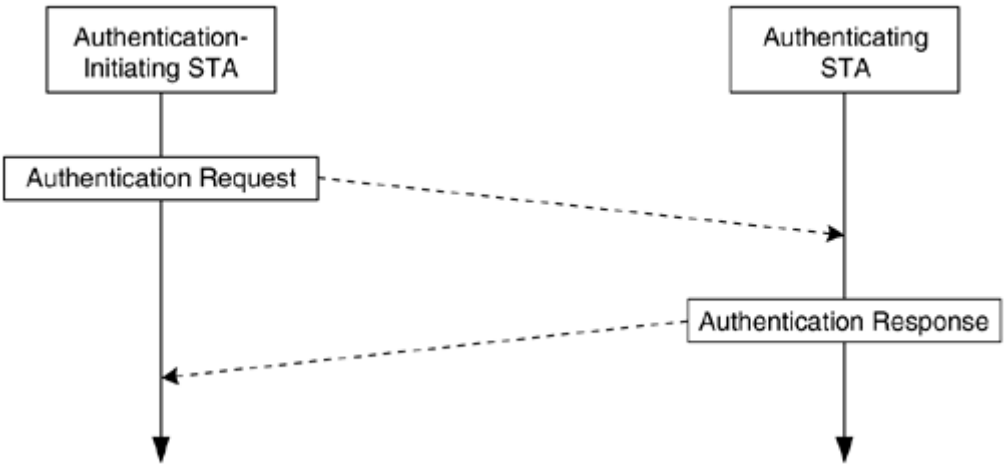

Figura 5-4: Negociação de autenticação *Open System*.

Cada mensagem, apesar de ter a mesma estrutura, transporta informação diferente, tal como mostrado na Figura 5-5, onde apenas se apresenta o campo de dados da trama, não se encontrando representado o cabeçalho da trama MMPDU nem o FCS (Figura 4-30).

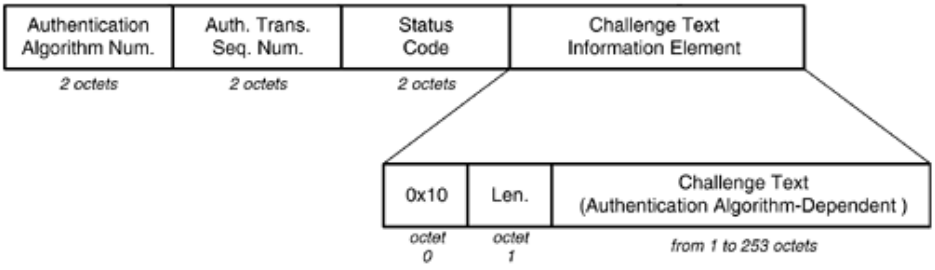

Figura 5-5: Dados de MMPDU de autenticação.

A primeira mensagem tem como objectivo iniciar o processo de autenticação *Open System* e provem da STA que se pretende autenticar, contendo a seguinte informação:

- *Authentication Algorithm Number*: 0 (*Open System*)
- *Authentication Transaction Sequence Number*: 1
- *Status Code*: 0 (Reserved)
- *Challenge Text*: Não está presente quando o *Authentication Algorithm Number* é zero.
- *Station Identity*: (obtida no campo *Source Address* (SA) do cabeçalho MMPDU)

A segunda mensagem é uma resposta da STA que confirma a autenticação sendo este tipo de frame apenas utilizada numa resposta de autenticação, e contem os seguintes campos:

- *Authentication Algorithm Number*: 0 ("Open System")
- *Authentication Transaction Sequence Number*: 2
- *Status Code*: (Resposta com sucesso ou outro da tabela 1)
- *Challenge Text*: Não está presente quando o *Authentication Algorithm Number* é zero.

A lista completa dos valores possíveis para o *Status Code* está descrita na Tabela 5-1:

Tabela 5-1: *Status Code* numa frame MMPDU de autenticação

Status Code	Significado
0	Successful
1	Unspecified failure
2 – 9	Reserved
10	Cannot support all requested capabilities in the Capability Information field
11	Reassociation denied due to inability to confirm that association exists
12	Association denied due to reason outside the scope of this standard
13	Responding station does not support the specified authentication algorithm
14	Received an Authentication MMPDU with authentication transaction sequence number out of expected sequence
15	Authentication rejected because of challenge failure
16	Authentication rejected due to timeout waiting for next frame in sequence
17	Association denied because AP is unable to handle additional associated STAs
18	Association denied due to requesting STA not supporting all of the data rates in the BSSBasicRateSet parameter
19 – 65,535	Reserved

Os valores do *Status Code* definidos na norma IEEE 802.11 que podem ser utilizados na mensagem de autenticação *Open System* são os números 0,1,12,13,15 ou 16. É também possível que a STA autenticadora recuse a autenticação (por exemplo em AP com validação por

endereço MAC), devendo devolver um *Status Code* com valor 13. A tabela apresenta também *Status Code* de tramas de associação.

5.3.2. Autenticação "*Shared Key*"

O processo utilizado na autenticação *Shared Key* é semelhante ao utilizado na autenticação *Open System*. A autenticação *Shared Key* especificada no IEEE 802.11-1997 e nas versões seguintes, refere-se ao facto de todas as STA partilharem o mesmo conhecimento da chave (ou chaves), que lhes permite ligar-se à WLAN. O processo de troca das quatro tramas de autenticação é mostrado na Figura 5-6.

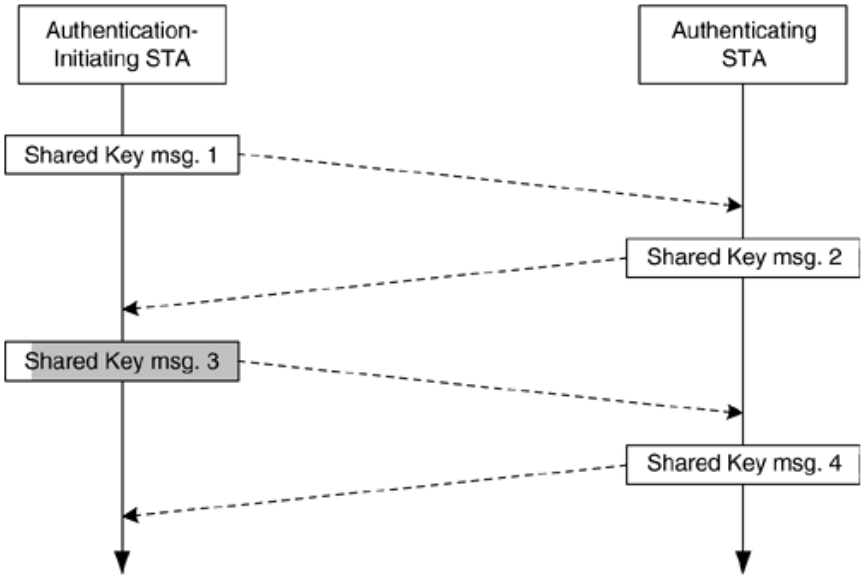

Figura 5-6: Negociação de autenticação Shared Key.

O formato das mensagens de autenticação *Shared Key* é idêntico ao utilizado na autenticação *Open System*. A grande diferença reside no facto de a autenticação *Shared Key* utilizar o campo *Challenge Text Information Element* ao contrário do que acontece na autenticação *Open System*. O campo *Challenge Text Information Element* poderá conter até um máximo de 253 bytes, sendo necessários apenas 128 por forma a negociar a autenticação *Shared Key*.

Em todas as mensagens de autenticação MMPDU utilizadas no *Shared Key* têm o campo *Type* com o valor "00" (Gestão) e o *SubType* com o valor "1101" (Autenticação) conforme figura 31.

5.3.2.1. Primeira trama de autenticação *Shared Key*

A primeira mensagem tem como objectivo iniciar o processo de autenticação *Shared key*, provém da STA que se pretende autenticar (*requester*), e contem a seguinte informação:

- *Authentication Algorithm Number* = 1 (Shared Key)
- *Authentication Transaction Sequence Number*: 1
- *Status Code: Reserved* (colocado a 0)
- *Challenge Text*: Não está presente nesta mensagem
- *Station Identity*: obtida no campo *Source Address* (SA) do cabeçalho MMPDU

5.3.2.2. Segunda trama de autenticação *Shared Key*

A segunda mensagem é uma resposta da STA (*responder*) que confirma a autenticação. Se o campo *Status Code* for diferente de "*Successful*", indica que não foi aceite a autenticação *Shared Key* devido a diversas razões e terminando neste ponto o processo de autenticação. A segunda mensagem (de resposta) de autenticação *Shared Key* e contem os seguintes campos:

- *Authentication Algorithm Number* = 1 (*Shared Key*)
- *Authentication Transaction Sequence Number*: 2
- *Status Code*: (Resposta com sucesso ou outro da tabela 1)
- *Challenge Text*: Texto com 128 bytes produzidos pelo gerador de números pseudo-aleatório do WEP e independente do valor de inicialização (IV) e da chave.
- *Station Identity*: (obtida no campo *Source Address* (SA) do cabeçalho MMPDU)

5.3.2.3. Terceira trama de autenticação *Shared Key*

Para a construção da terceira mensagem a STA *requester* deverá copiar o *Challenge Text* obtido da segunda trama para o mesmo campo na terceira trama e preencher os outros campos como se segue:

- *Authentication Algorithm Number* = 1 (Shared Key)
- *Authentication Transaction Sequence Number*: 3
- *Status Code: Successful* (colocado a 0)
- *Challenge Text*: Texto com 128 bytes copiado da segunda trama.
- *Station Identity*: (obtida no campo *Source Address* (SA) do cabeçalho MMPDU)

Esta trama será enviada depois de cifrada utilizando o protocolo WEP.

5.3.2.4. Quarta trama de autenticação *Shared Key*

O receptor da terceira trama (STA *responder*) poderá obter do cabeçalho WEP qual a chave utilizada para cifrar a trama, e se conseguir decifrar a trama poderá verificar se o *Challenge Text* que obtém é o mesmo que o enviado na segunda trama. Conforme será descrito posteriormente o WEP utiliza-se o algoritmo CRC-32 para produzir o *Integrity Check Value* (ICV) que serve para validar a integridade da mensagem.
O facto da terceira mensagem vir cifrada apenas prova que a STA a *responder* conhece a chaves WEP, sendo uma barreira de defesa fraca, como se descreverá mais tarde.
A quarta trama do processo de autenticação *Shared Key* é a confirmação que a STA de autenticação recebeu a terceira trama e que autoriza a STA *requester* a utilizar a BSS (seja em modo infra-estrutura sejam no modo IBSS) e contém os seguintes campos:

- *Authentication Algorithm Number* = 1 (Shared Key)
- *Authentication Transaction Sequence Number*: 4
- *Status Code: Successful* ou *unsuccessful* (dependendo da validação do ICV)
- *Station Identity*: (obtida no campo *Source Address* (SA) do cabeçalho MMPDU)

5.3.3. Processo de associação de uma STA a um AP.

O processo de associação é bastante simples e consiste apenas na troca de duas mensagens entre a STA e o AP. Relembra-se que uma STA poderá estar autenticada em vários AP simultaneamente mas que apenas poderá estar associado a um de cada vez. Só depois de estar associado é que uma STA poderá enviar e receber dados de outras STA através do AP.
Existem três tipos de mensagens para o processo de associação: "*Association*", "*Re-Association*" e "*Disassociation*". A primeira serve para estabelecer uma associação entre uma STA e um AP, a segunda mensagem serve para alterar os parâmetros de uma associação existente ou para mover uma STA para outro AP (que já esteja autenticado).

O processo de associação que ocorre depois do processo de autenticação consiste na troca de duas mensagens, *Association Request* (STA para o AP) e *Association Response* (resposta do AP para a STA).

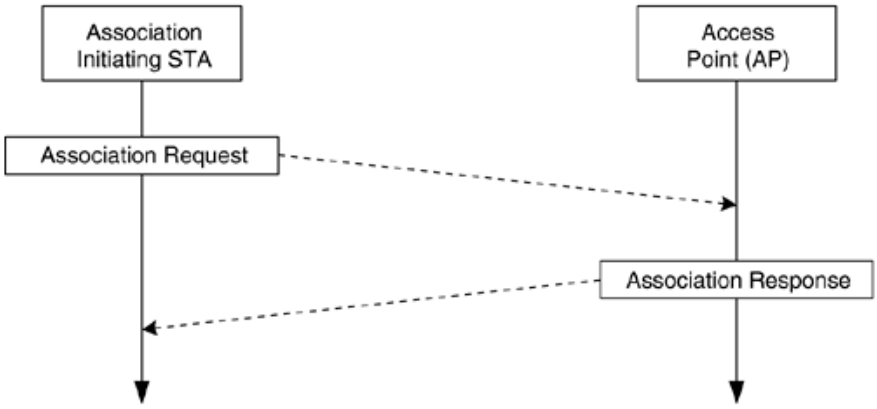

Figura 5-7: Processo de associação entre a STA e o AP.

Este processo é implementado através de tramas de gestão (MMPDU) (Figura 5-8) podendo as tramas conter no seu campo de dados informação variada.

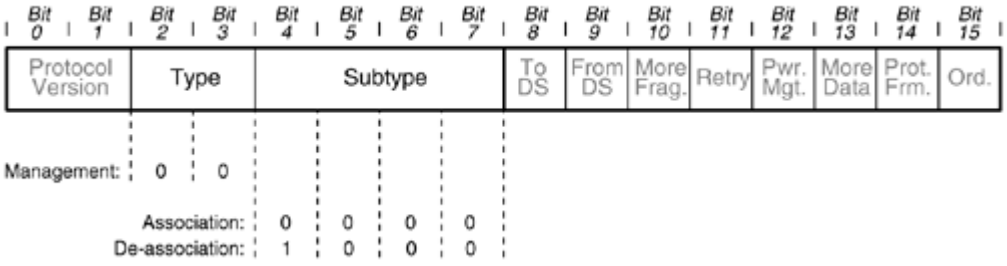

Figura 5-8: Campo *Frame Control* de um MMPDU no processo de associação.

5.3.3.1. Tramas de associação *Association Request*

Cada trama de *Association Request* (Figura 5-8) contém os seguintes campos:

- Identificação da STA: Obtém-se a partir do campo *Source Address* (SA) do cabeçalho do MMPDU.
- Identificação do AP: Obtém-se a partir do campo *Destination Address* (DA) do cabeçalho do MMPDU.
- ESS Id: (Assegura que a STA se associa à WLAN correcta). O SSID é uma cadeia de texto que representa o nome de uma rede. A estação que necessita de se juntar à rede necessita de saber esta informação que seja introduzida manualmente que seja obtida automaticamente através das tramas *beacon*.

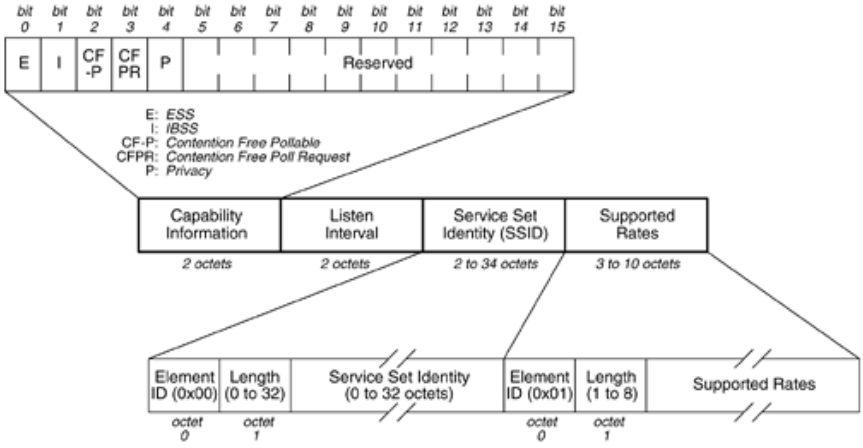

Figura 5-9: Conteúdo de uma trama MMPDU *Association Request*.

Na *trama* de *Association Request* aparecem diversos tipos de informação adicional como sejam qual o modo de funcionamento ESS ou IBSS, se processo de Privacidade está activo na WLAN, se a STA suporta o funcionamento de *Contention-Free* (PCF) e as velocidades de transmissão a que pode funcionar a STA. O AP utiliza esta informação para determinar se aceita a associação. A STA poderá também informar o AP da duração do "*Listen Interval*" que representa a quantidade de tempo que a STA fica no modo *power-saving*, expressa em unidades de intervalos *Beacons* (a STA poderá entrar em "*sleep*" em intervalos de 1 a 65535 unidades *Beacon*).

5.3.3.2. Tramas de associação *Association Response*

A mensagem de *Association Response* (Figura 5-10) é enviada pelo AP para a STA se a associação proposta for aceite. Esta trama de gestão MMPSU é apenas utilizada em resposta a uma trama *Association Request* e contém a seguinte informação:

- *Association Identifier*. O *Association ID* é um número de 14 bits cujo valor pode situar-se no intervalo de 1 a 2007. Os dois primeiros bits do campo *Association ID* (16 bits) são colocados a 1. Este número é atribuído pelo AP para referenciar a associação criada. A única outra trama que contem o campo *Association ID* é a trama de controlo *Power-Save Poll*, que o AP utiliza para indicar à STA que tem dados que lhe são destinado na *queue* do AP.
- O AP devolve a lista das velocidades de transmissão que suporta, para que a STA possa limitar a sua transmissão pela intersecção com as suas próprias velocidades suportadas.
- *Status Code*. O *Status Code* deverá ser escolhido de acordo com as condições de resposta ao pedido de associação.

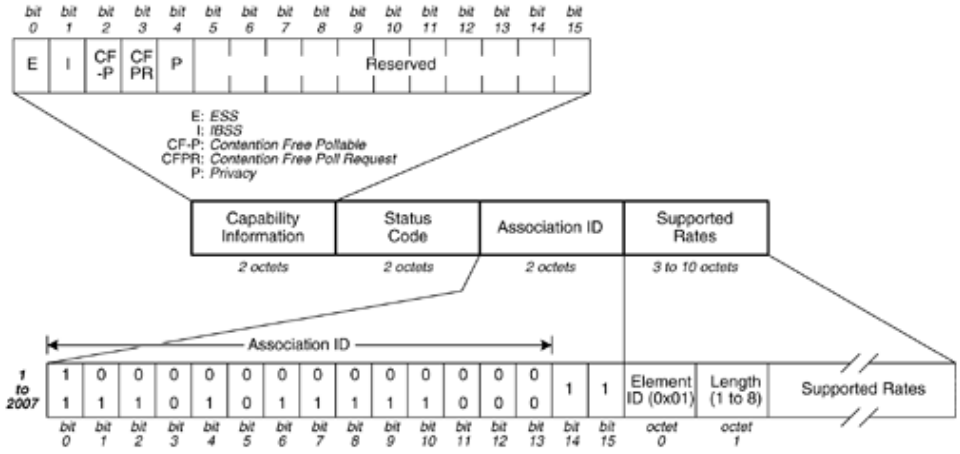

Figura 5-10: Formato de uma trama MMPDU *Association Response*.

Logo que terminado o processo de associação a STA poderá enviar tramas para qualquer outra STA que esteja ela associada ao AP (BSS) ou via DSS (a rede com fios que liga os APs do ESS).

5.4. Serviços de confidencialidade

A norma IEEE 802.11 implementa as características de confidencialidade através da utilização de técnicas criptográficas na transmissão de ramas. A primeira técnica criptográfica definida foi o WEP que, para proporcionar confidencialidade, definia a utilização do algoritmo de cifra RC4 de chaves simétricas que funciona em modo continuo para produzir uma sequência de dados pseudo-aleatórios, interceptados através de uma operação lógica exclusive-OR com os dados reais que se pretendem transmitir. Através do WEP os dados podem ser protegidos durante a transmissão na rede sem fios.

5.5. Serviços de integridade

A norma IEEE 802.11 inicial especificava um meio de proporcionar integridade para os dados existentes nas mensagens transmitidas entre as STA e os APs. Este serviço de segurança foi desenhado para rejeitar qualquer mensagem que for alterada por algum meio durante a transmissão. A técnica especificada consistia na utilização de *Cyclic Redundancy Check* (CRC) sobre os dados e que depois é enviado (juntamente com os dados) cifrado. No lado do receptor, depois de decifrada a trama é recalculado o CRC dos dados recebidos. Se o CRC obtido for diferente daquele que vem na mensagem, indica que houve uma violação da integridade da trama e esta não será processada. O mecanismo de CRC não é um mecanismo criptograficamente seguro e como tal apresenta muitas vulnerabilidades (6.2.1).

5.6. Wired Equivalent Privacy (WEP)

5.6.1. Introdução ao WEP

A norma IEEE 802.11 de 1997 incluía um mecanismo opcional de privacidade para proporcionar um nível de protecção equivalente ao existente numa rede com fios, que se manteve na versão da norma de 1999.
Uma das maiores criticas apontadas ao WEP é o facto de não proporcionar nenhum mecanismo de troca de chaves de cifra, e assumir que estas foram distribuídas de forma segura a cada um dos nós da rede através de outros meios. Havendo necessidade de distribuir manualmente as chaves a cada um dos dispositivos da rede, significa de o WEP não permite um crescimento sustentado de nós em redes de grande dimensão e que, ou por políticas de alteração de chaves ou por comprometimento das mesmas, a substituição das chaves nessas redes é um trabalho penoso e demorado, podendo expor a rede a ataques desnecessários.

O IEEE 802.11 define um mecanismo para cifrar o conteúdo das tramas de dados. Este esquema utiliza seis elementos directamente relevantes para a sua análise:

- Uma chave partilhada entre todos os membros do BSS (na realidade existem quatro chaves, mas são irrelevantes para o mecanismo).
- Um algoritmo de cifra. Para o WEP o RC4 é utilizado para a geração de uma *stream* de cifra, que será interceptada com a mensagem a claro através de uma operação XOR produzindo uma mensagem cifrada.
- Um algoritmo para decifrar a mensagem. Para o WEP é utilizado o mesmo algoritmo de RC4, que com a mesma chave de cifra produz uma *stream* que será também interceptada com a mensagem recebida cifrada através de uma operação XOR produzindo a mensagem a claro.
- Um vector de inicialização (IV) de 24 bits. O WEP acrescenta o IV à chave partilhada produzindo uma chave única que servirá de entrada ao RC4 para a produção da *stream* de cifra. O WEP selecciona um IV por cada pacote.
- Um encapsulamento que transporta o IV e a mensagem cifrada desde o emissor até ao receptor.
- Um mecanismo de integridade de dados. O WEP calcula o CRC da mensagem em claro que é acrescentada no fim da mensagem antes de ser cifrada.

As chaves são simétricas e o processo de cifra compreende a concatenação da chave com um vector (IV) de 24 bits resultando numa sequência de 64 ou 128 bits que serve de *entrada* (*seed*) ao algoritmo *Ron Code 4* (RC4) *Pseudo Random Number Generator*. O resultado obtido é utilizado para a cifra dos dados.

O WEP é um mecanismo de segurança da norma 802.11, proporcionando cifra das comunicações, baseada numa partilha de chaves WEP com 40 ou 104 bits entre o AP e as estações.
A norma 802.11 não especifica um protocolo de gestão de chaves pelo que qualquer alteração de chaves terá que ser feita manualmente, tornando difícil a gestão. Este mecanismo tem fraquezas: ao nível da autenticação pois apenas o cliente é autenticado pelo AP (e não o inverso), permitindo ataques do tipo "*man-in-the-middle*"; as chaves reutilizadas e facilmente decifráveis, normalmente estáticas, o vector IV transmitido em claro existindo já inúmeras ferramentas para decifra as chaves como sejam WEPCrack ou AirSnort [5].

5.6.2. Descrição do funcionamento do WEP.

Cada STA que pretenda ligar-se à rede terá que obter a chave partilhada (40 bits ou 104 bits) por um meio manual, uma vez que a norma IEEE 802.11 não especifica nenhum mecanismo de distribuição de chaves.
O formato da parte de dados de uma trama cifrada WEP está descrito na Figura 5-11. A mensagem original (MPDU) é expandida em 8 bytes. Quatro bytes são adicionados no início do PDU (Dados) e representam o vector de inicialização (IV) e os outros quatro bytes são adicionados no fim do PDU para criar o valor de validação de integridade (*integrity check value* - ICV). Os quatros bytes que compreendem o IV são construídos com um vector de inicialização de 24 bits, seguidos de seis bits reservados e terminando em dois bits para índice da chave de cifra utilizada *Key ID* (o WEP permite a utilização de quatro chaves estáticas num BSS; uma estação transmite utilizando apenas uma das chaves, a *default key*, mas deve poder receber dados cifrados em qualquer uma das quatro chaves; o *Key ID* identifica com qual das quatro chaves foi cifrada a mensagem).

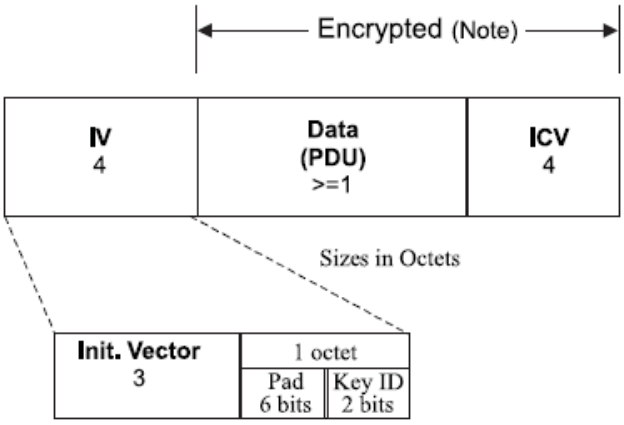

Figura 5-11: Formato do corpo uma trama WEP.

O vector de inicialização de 24 bits proporciona duas funções: é o mecanismo com o qual as novas cifras são geradas a cada trama a transmitir e proporciona a sincronização no processo de cifra/decifra entre o emissor e o receptor em caso de perda ou retransmissão de pacotes. O ICV é um *checksum* CRC-32 aplicado sobre os dados a claro (não cifrados) que é acrescentado a própria mensagem e que incluída no processo de cifra. O ICV permitirá ao receptor determinar se a trama recebida sou alterada durante a transmissão.

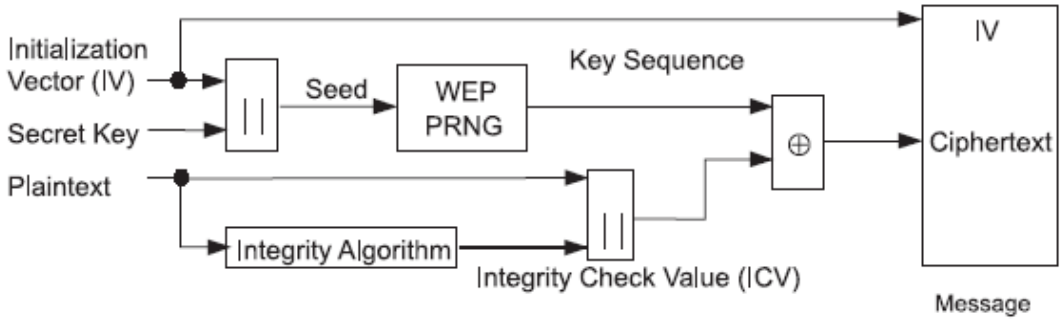

Figura 5-12: Diagrama de blocos de cifra WEP.

O processo de encapsulamento WEP é mostrado na Figura 5-12. O vector de inicialização de 24 bits é concatenado com a chave secreta estática (40-bits ou 104 bits) para formar a semente (64-bits ou 128-bits) que é utilizada na inicialização do bloco de cifra *Ron Code 4* (RC4) *Pseudo Random Number Generator*.. O IV deverá ser único para cada pacote, sendo esta a recomendação do IEEE 802.11. Em algumas implementações este campo é apenas um contador incrementado a cada pacote. A cifra RC4 cria uma sequência de bits aleatória (*keystream*) que combinada com os dados numa operação XOR cria uma mensagem cifrada. A operação final consiste na colocação do IV à cabeça da mensagem cifrada e este conjunto (Figura 5-13) é transmitido pelo emissor. A indicação de que uma trama está cifrada é feita através da activação da *flag Protected Frame* no campo *Frame Control* (FC) no cabeçalho da trama.

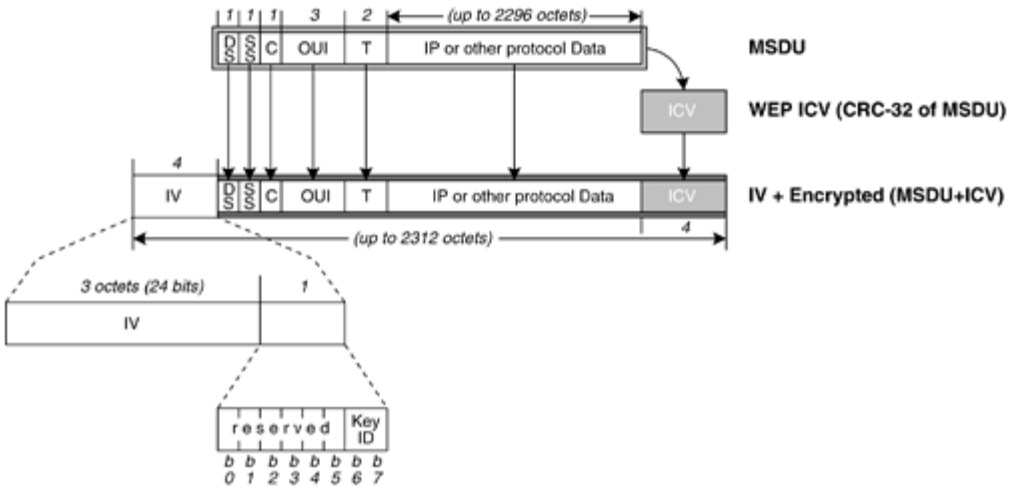

Figura 5-13: Detalhe do corpo de mensagem cifrada com WEP.

Para processar a trama WEP o receptor verifica primeiro se está cifrada através da *flag Protected Frame* no campo *Frame Control* (FC). O receptor extrai do início da trama cifrada o vector de inicialização de 24 bits (IV) e o índice da chave (das quatro) que foi utilizada para cifrar a mensagem. A concatenação do IV com a chave secreta estática forma a semente utilizada na inicialização do bloco de cifra *Ron Code 4 (RC4) Pseudo Random Number Generator* (Figura 5-14).

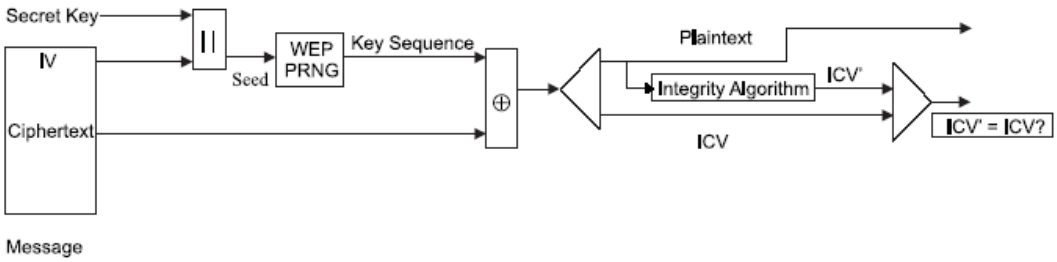

Figura 5-14: Diagrama de blocos de decifra WEP.

A cifra RC4 cria uma sequência de bits aleatória (*keystream*) que combinada com os dados cifrados numa operação XOR produz a mensagem original a claro. O receptor verifica a integridade da mensagem ao calcular o ICV através de uma função CRC-32 que irá comparar com o valor ICV obtido na trama decifrada.

5.7. IEEE 802.11i

Tal como descrito anteriormente e em (6.2.1), a segurança das redes sem fios baseada em WEP é facilmente ultrapassável. Devido às vulnerabilidades descobertas foi criado o *IEEE 802.11 Task Group "i" (TGi)* com o objectivo de criar uma evolução no modelo de segurança que viesse endereçar as fraquezas identificadas. O IEEE 802.11i [37] também conhecido como WPA2, define para a cifra dos dados o protocolo ***Temporal Key Integrity Protocol (TKIP)*** e o protocolo ***CBC-MAC em Counter Mode (CCMP)*** baseado no ***Advanced Encryption Standard (AES-128)***, mecanismo de gestão de chaves, descoberta e negociação de componentes de segurança e especifica a possibilidade de utilização de componentes (protocolos) externos de autenticação como seja o ***IEEE 802.1X port-based authentication***.

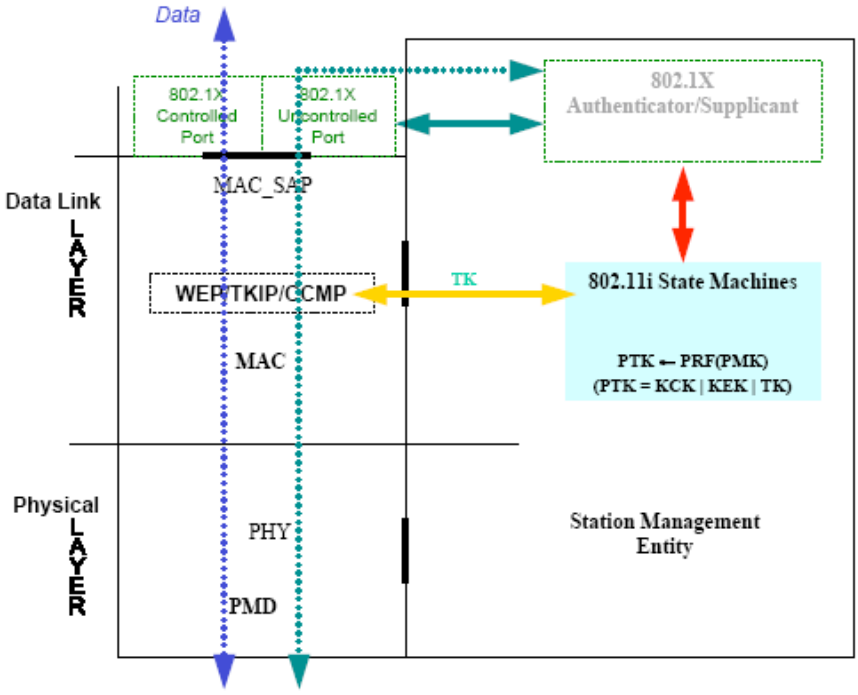

Figura 5-15: Arquitectura do IEEE 802.11i.

O IEEE 802.11i contempla aspectos de segurança para redes sem fios em modo infra-estrutura (BSS) e em modo *ad-hoc* (IBSS) e baseado na sua especificação (desde o Draft) apareceram os modelos Wi-Fi Protected Access (WPA) e Robust Security Network (RSN) ou WPA2.

5.7.1. Wi-Fi Protected Access (WPA)

O protocolo WPA é baseado na norma 802.11i (versão *draft*). Utilizando os mecanismos de autenticação IEEE 802.1X para corrigir ao problemas de segurança sobre as chaves do WEP, incluía do IEEE 802.11i o protocolo *Temporary Key Integrity Protocol* (TKIP) para o processo de cifra, colmatando as fragilidades existentes no WEP:

- Chaves dinâmicas (permite chaves dinâmicas por utilizador e por sessão);
- *Message Integrity Checking* (MIC) para garantir que a mensagem não é alterada durante a transmissão;
- Aumento do vector de inicialização IV de 24 para 48 bits, possibilitando melhoria no algoritmo de cifra e um aumento do tempo de repetição do vector
- Correcção de vulnerabilidades associadas ao envio a claro do vector de inicialização IV.

Para além do TKIP, na sua versão inicial de Novembro de 2002, a norma IEEE 802.11i incluía também as funcionalidades de algoritmos de gestão de chaves, processo de negociação de autenticação e cifra.

5.7.2. Robust Security Network (RSN)

O *Robust Security Network* (RSN) é o nome utilizado para identificar as redes sem fios que utilizam a norma final IEEE 802.11i. A segurança da RSN compreende dois subsistemas:

- Gestão de associação de segurança
    - Procedimentos de negociação para estabelecimento de um contexto de segurança.
    - Substituição do mecanismo de autenticação do IEEE 802.11 por um outro como seja o IEEE 802.1X
- Mecanismos de privacidade dos dados
    - TKIP
    - CCMP (Protocolo baseado no AES -128)

Utilizando mecanismos de negociação dinâmica, 802.1X, EAP e AES, o RSN é significativamente mais robusto que o WEP ou o WPA.
Como o processo de transição para uma rede RSN pura é evolutivo, foi definida uma *Transitional Security Network* (TSN) onde se admite numa rede sem fios a utilização em paralelo de RSN e WEP.

5.7.3. Temporal Key Integrity Protocol (TKIP)

O TKIP [37] foi desenhado dando respostas às fragilidades da cifra existente nos algoritmos do WEP, tendo também como objectivo poder ser utilizado nos equipamentos Wi-Fi (*hardware*) que já utilizavam WEP. O TKIP traz múltiplas melhorias ao mecanismo de cifra do WEP: utilização de chaves dinâmicas (chaves dinâmicas por utilizador e por sessão); acrescentado o campo *Message Integrity Checking* (MIC) de 8 bytes a cada mensagem (Figura 5-16) para garantir que não é alterada durante a transmissão; aumento do vector de inicialização IV de 24 para 48 bits, possibilitando melhoria no algoritmo de cifra e um aumento do tempo de repetição do vector; correcção de vulnerabilidades associadas ao envio a claro do vector de inicialização IV; mecanismos de protecção de repetição de mensagens através de detecção de ordenação de sequência de transmissão.

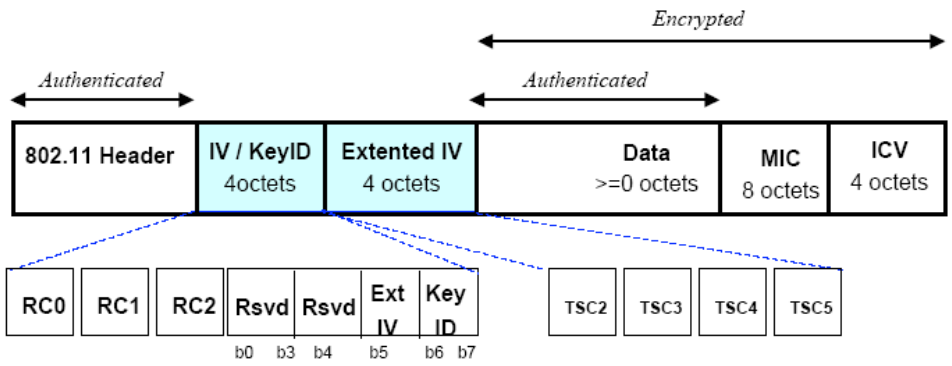

Figura 5-16: TKIP – Formato da MPDU.

A estrutura de um MPDU cifrado utilizando TKIP é mostrada na Figura 5-16. O TKIP utiliza um vector de inicialização de 48 bits chamado de *TKIP Sequence Counter* (TSC). A utilização do TSC de 48 bits aumenta o tempo de vida da chave temporal (descrita mais à frente) e elimina a necessidade de reatribuição de novo valor à chave temporal durante uma associação (uma vez que o TSC é actualizado por cada pacote, poderão ser transmitidos 2^{48} pacotes antes que a chave volte a repetir-se). O TSC é construído com base nos primeiro e último bytes do WEP IV e nos 4 bytes proporcionados pelo IV acrescentado. O TKIP aumenta em 12 bytes o tamanho do MPDU; 4 bytes para o *Extended IV* e 8 bytes para o *MIC*.

O processo de encapsulamento do TKIP mostrado na Figura 5-17 mostra como as chaves MIC e Temporal são utilizadas. Estas chaves são produzidas a partir da *Pairwise Master Key* (PMK) que foi gerada como parte do processo IEEE 802.1X. A chave *Temporary Key*, o endereço de

transmissão e o TSC são combinados através de uma função (*Key Mixing*) para produzirem uma chave por cada pacote que será usada como semente (*seed*) para o processo de cifra do WEP. A chave produzida tem 128 bits que são repartidos respectivamente pela chave do RC4 de 104 bits e pelo IV de 24 bits.

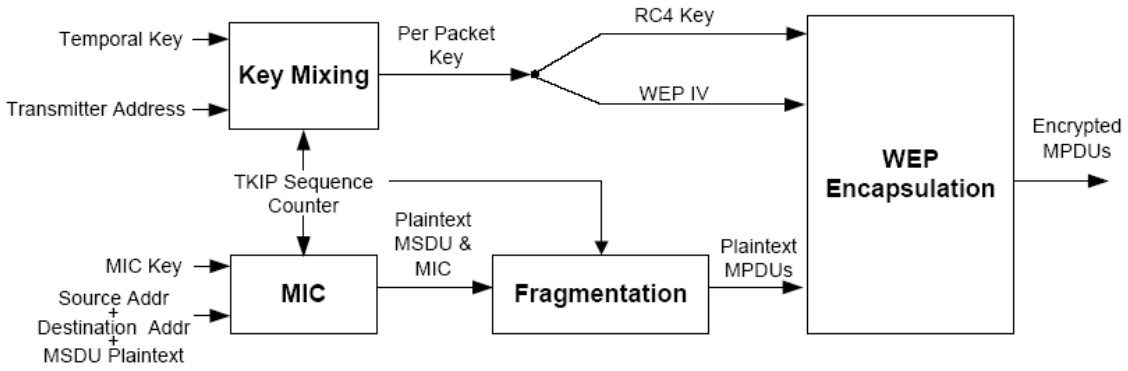

Figura 5-17: TKIP – Processo de Encapsulamento.

O MIC é calculado utilizando os endereços MAC da origem e destino, e os dados em claro. Ao utilizar os endereços da origem e do destino o MPDU fica protegido contra ataques de alteração de dados em trânsito. A função MIC, também chamada de *Michael*, é uma operação criptográfica *hash one-way*, e não um simples CRC-32 utilizado no WEP ICV. O resultado de alteração de dados dos pacotes irá apenas corresponder a um ataque tipo *deny of service* (DoS).
O processo de desencapsulamento é semelhante ao de encapsulamento. Depois de se obter o TSC do pacote recebido, é examinado para verificar que o TSC recebido é superior ao do pacote anterior. Caso não seja o pacote, é ignorado por forma a prevenir ataques de reenvio de pacotes. Depois de decifrado o pacote é calculado o MIC correspondente e comparado com o MIC existente no pacote. Se forem diferentes o pacote é ignorado e poderão ser iniciadas contramedidas como a recriação da chave Temporal e a notificação de um administrador de rede.

5.7.4. AES: Counter Mode with CBC-MAC Protocol (CCMP)

Para além do mecanismo de cifra TKIP, que foi desenhado para resolver as vulnerabilidades do WEP, o IEEE 802.11i definiu um novo método de cifra por blocos baseado no *Advanced Encryption Standard* (AES), o protocolo *Counter Mode with* CBC-MAC (CCMP) [37]. Ao contrário do TKIP o CCMP envolve a substituição total do WEP, visto que não foi desenhado para ser compatível com protocolos anteriores, obrigando em muitos casos a substituição do *hardware* dos dispositivos wireless devido a maiores necessidades de processamento.

O AES pode ser utilizado em diferentes modos ou algoritmos. O modo escolhido para o IEEE 802.11 é o CCMP. O *Counter Mode* proporciona privacidade nos dados enquanto que o CBC-MAC (*Cyber Block Chaining Message Authentication Code*) proporciona integridade e autenticação dos dados.

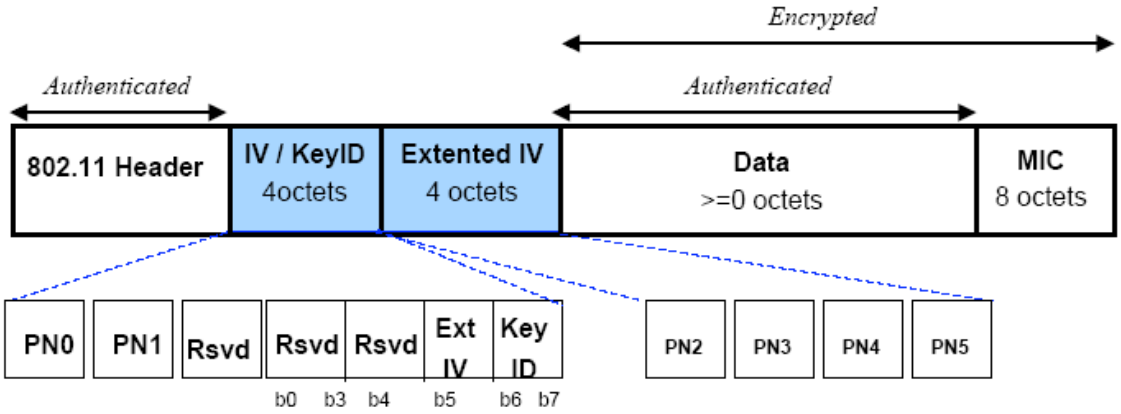

Figura 5-18: CCMP – Formato da MPDU.

O formato do pacote MPDU é mostrado na Figura 5-18. O pacote é aumentado de 16 bytes e tem um formato idêntico ao do TKIP com excepção de não ter o WEP ICV. Tal como o TKIP, o CCMP utiliza um IV de 48 bits chamado de *Packet Number* (PN). O PN é utilizado para inicializar o cálculo do MIC e a cifra da mensagem.

O AES é um processo de cifra simétrico por blocos, significando que é utilizada a mesma chave para cifrar e decifrar, onde cada unidade de cifra é um bloco de tamanho fixo extraído da mensagem original. A norma AES utiliza blocos de 128 bits para a cifra, e o mesmo valor foi adoptado para o IEEE 802.11.

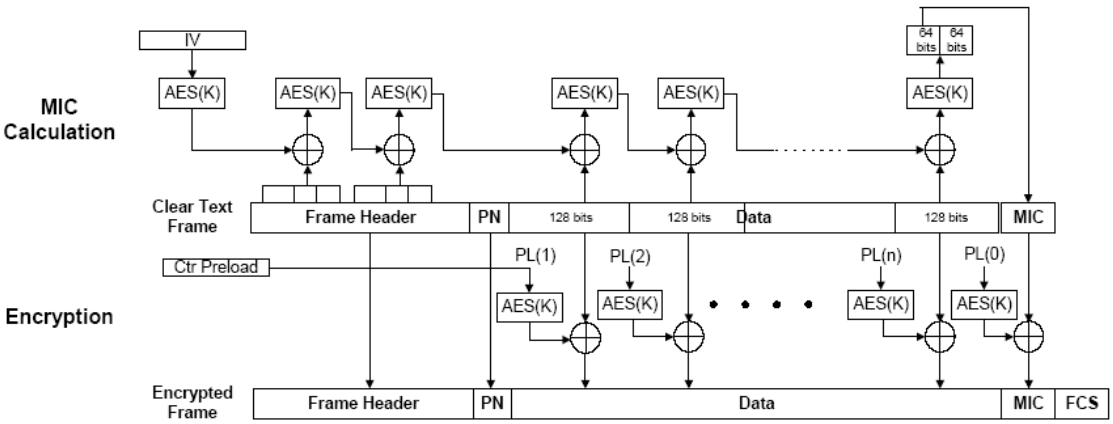

Figura 5-19: CCMP – Processo de encapsulamento.

É utilizada a mesma chave temporal de cifra (K na Figura 5-19), para cifrar e calcular o MIC nos blocos AES. Tal como no TKIP a chave temporal é produzida a partir da *Pairwise Master Key* (PMK) que foi gerada como parte do processo IEEE 802.1X. O cálculo do MIC e o processo de cifra seguem caminhos paralelos até ao processamento completo dos dados, calculando-se o valor final do MIC a ser inserido na mensagem.

O processo de desencapsulamento é o inverso ao do encapsulamento. Depois de decifrado o pacote e calculado o MIC é efectuada a comparação com o MIC existente no pacote. Se forem diferentes o pacote é ignorado.

5.8. Protocolo de autenticação IEEE 802.1X *port-based authentication*

Tal como já referido os protocolos de autenticação não estão especificados na norma IEEE 802.11i [37], mas fazem parte integrante do modelo de segurança. Existem diversos protocolos de autenticação utilizados actualmente, normalmente em ambientes empresariais, que proporcionam autenticação mútua dos intervenientes, identificadores de sessão e geração de chaves de sessão que podem ser utilizadas nas redes sem fios entre o dispositivo cliente e o AP.

A norma IEEE 802.1X [38] [39] é utilizada como um método normalizado de controlo de acessos, autenticação e gestão de chaves.

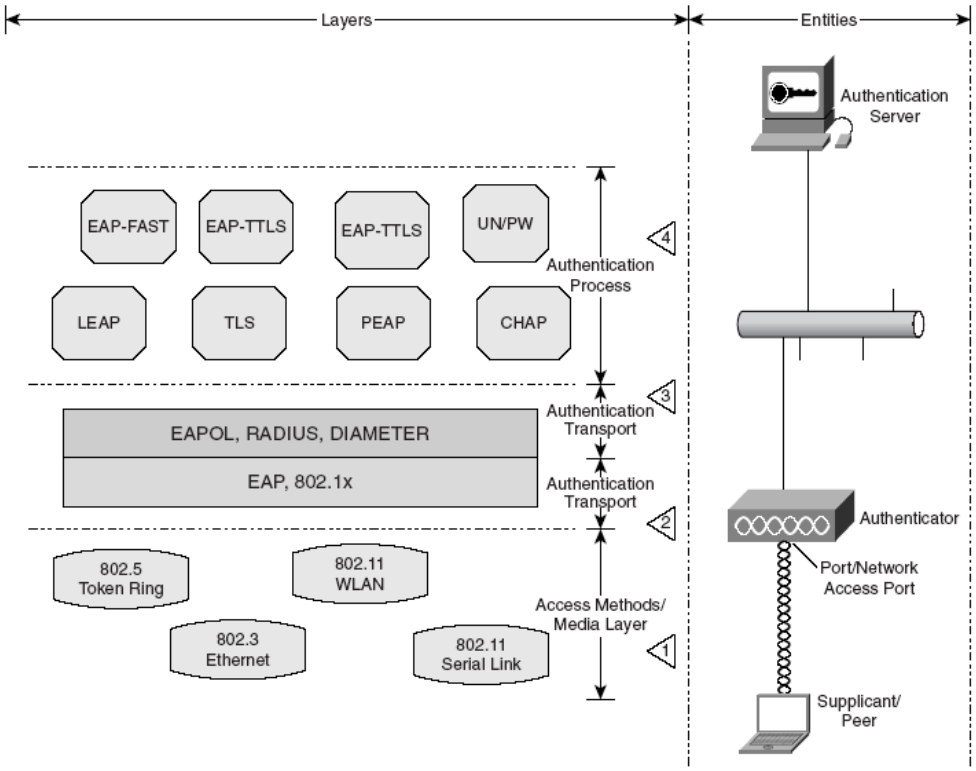

Figura 5-20: IEEE 802.1X – Layers e Entidades [40]

O IEEE 802.1X divide o universo da rede em três entidades (Figura 5-20):

- ***Supplicant***

  O utilizador ou o dispositivo cliente que quer ser autenticado. O *Supplicant* acede aos serviços de autenticação através do *Authenticator* utilizando o protocolo EAP over LAN (EAPOL).

- ***Authenticator***

  Tipicamente reside em qualquer AP (ou um *switch* em redes com fios) com funcionalidades 802.1X. O *Authenticator* controla o acesso físico à rede baseado no estado de autenticação do *Supplicant*. Ao receber as mensagens EAPOL reencaminha-as para um *Authentication Server* utilizando o protocolo EAP over RADIUS.

- ***Authentication Server***

  Tipicamente corresponde a um servidor RADIUS [34] que fornece os serviços de autenticação a um *Authenticator*. Através das credenciais fornecidas pelo *Supplicant*, este serviço determina se o *Supplicant* é autorizado a aceder aos serviços fornecidos pelo *Authenticator*.

Estas entidades são entidades lógicas nos dispositivos. O *Authenticator* cria uma porta lógica por cada cliente baseado no identificador de associação AID (*Association* ID). Esta porta lógica tem dois caminhos – um sem controlo e outro controlado (Figura 5-21). O caminho sem controlo filtra todo o tráfico excepto mensagens de autenticação (EAPOL). O caminho controlado irá permitir todo o tráfico depois de o cliente se ter autenticado com sucesso.

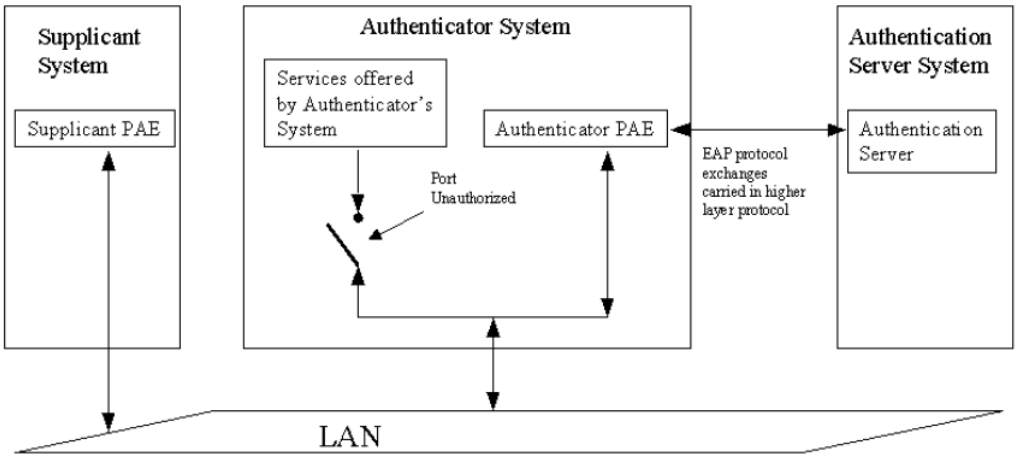

Figura 5-21: IEEE 802.1X – Modelo de controlo de acesso

5.8.1. Processo de Autenticação EAP

O protocolo EAP suporta múltiplos métodos de autenticação. No entanto, o modo de funcionamento mostrado na Figura 5-22 é comum a todos eles.

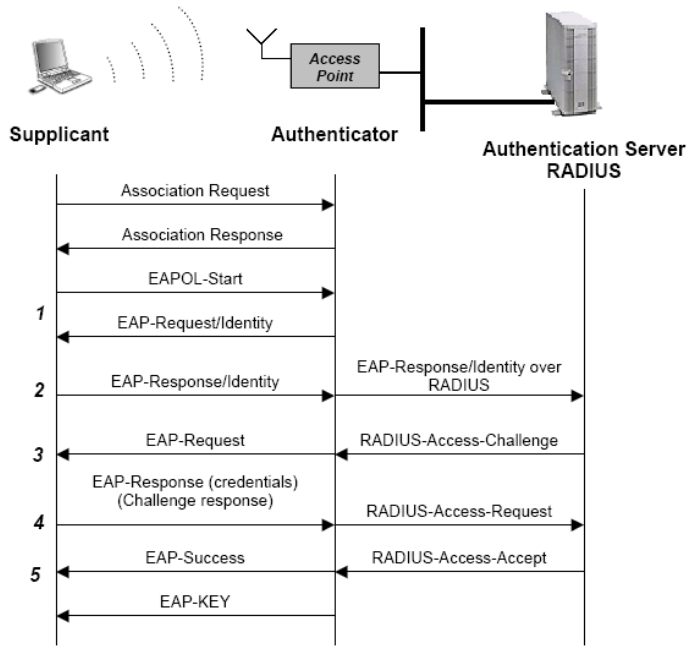

Figura 5-22: IEEE 802.1X EAP Authentication

É importante referenciar que antes de se iniciar o processo de autenticação EAP, um dispositivo cliente (STA) tem que efectuar o processo de autenticação e associação IEEE 802.11 com um AP (descrito em pontos anteriores).

O processo de autenticação EAP corresponde às seguintes fases:

1. Logo que uma estação (*Supplicant*) é associada ao *Access Point*, o *Authenticator* (no próprio AP) detecta a associação e disponibiliza uma porta ao *Supplicant*. A porta é forçada a um estado não autorizado para que apenas o trafico 802.1X seja autorizado e todo o outro tráfico seja bloqueado. Logo que o cliente inicia a comunicação EAPOL (*EAPOL-Start*). O *Authenticator* responde enviando um pacote *EAP-Request/Identity* para o *Supplicant* pedindo a identidade do cliente.
2. O *Supplicant* envia um pacote *EAP-Response/Identity* com a sua identificação para o *Authenticator*, que por sua vez o reenvia para o *Authentication Server* (RADIUS) encapsulado no protocolo RADIUS.

3. O *Authentication Server* responde com um desafio (*RADIUS-Access-Challenge*) para o *Authenticator*. O *Authenticator* transforma o desafio num pacote EAPOL e envia-o para o *Supplicant*.
4. O *Supplicant* responde ao desafio incluindo as suas credenciais (por exemplo a password ou o resultado de uma operação de cifra). Esta resposta é enviada para o *Authentication Server (RADIUS-Access-Request*) através do *Authenticator*.
5. Conforme o resultado da validação feita ás credenciais apresentadas pelo *Supplicant* assim o *Authentication Server* (RADIUS) responde com uma mensagem *RADIUS-Access-Accept* ou *RADIUS-Access-Reject*. Se a autenticação foi efectuada com sucesso, a mensagem RADIUS contem um atributo correspondendo à chave de sessão.
6. A porta lógica do *Authenticator* passa para um modo controlado permitindo todo o tráfico proveniente do *Supplicant*. Opcionalmente é enviada a chave de sessão para o *Supplicant* através de uma mensagem *EAPOL-Key*.

As fases 3 e 4 do processo de autenticação, consoante o método de autenticação seleccionado, poderão corresponder a diversas mensagens e possibilitando a autenticação mútua dos intervenientes bem como a criação de chaves de sessão partilhadas.

À máquina de estados do IEEE 802.11, com a utilização do IEEE 802.1X foi acrescentado um novo estado (Figura 5-23).

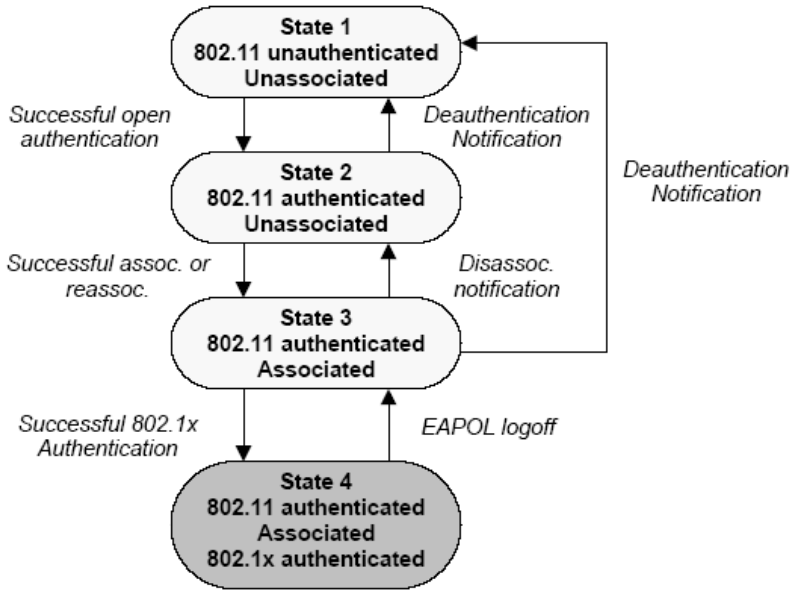

Figura 5-23: IEEE 802.11/802.1X - Máquina de estados

5.8.2. Formato de tramas EAP

Na Figura 5-20 mostra-se os vários *níveis* do protocolo 802.1X e pode-se ver que o protocolo EAP está situado ao nível *Transport* (no modelo OSI) possibilitando a implementação dos diversos métodos de autenticação (PEAP, LEAP, TLS, etc). As tramas que suportam o protocolo EAP (Figura 5-24) têm o seguinte formato:

- *Code* (1 Byte) – tipo de mensagem: (1) *Request*, (2) *Response*, (3) *Success*, (4) *Failure*.
- *Identifier* (1 Byte) – É um valor que deverá ser incrementado por cada mensagem. Quando uma resposta é enviada o valor do campo deve ser igual ao da mensagem de pedido.
- *Length* (2 bytes) – Campo que indica o tamanho da mensagem EAP incluindo os campos *Code, Identifier, Type e Data*.
- *Type* (1 Bytes) – Este campo só aparece nos pacotes de *EAP-Request* e *EAP-Response*. Pode assumir diversos valores: (1) Identidade (identificação do utilizador), (2) Notificação, (3) *Resquest Type* não suportado (resposta de NACK), valores superiores a (4) identificam um método de autenticação (por exemplo igual a 13 para o EAP-TLS).
- *Data* (variável) – Os dados dependem do método EAP utilizado.

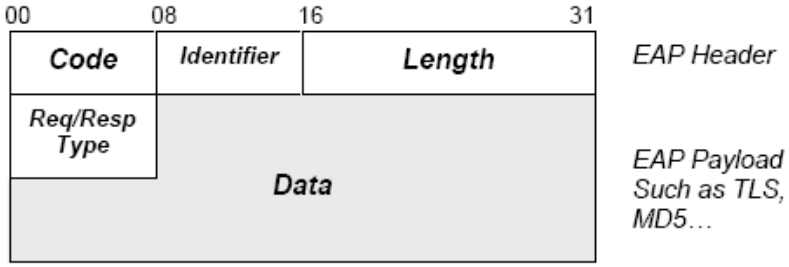

Figura 5-24: EAP – Formato da trama

5.8.3. Descrição dos tipos de autenticação EAP

Descrevem-se de seguida alguns dos métodos de autenticação mais utilizados.

5.8.3.1. EAP-Message Digest 5 (EAP-MD5)

O EAP-MD5 é um dos mais simples métodos de autenticação. O algoritmo MD5 (RFC 1321) tem como parâmetros de entrada uma mensagem de tamanho variável e uma *password*, e como resultado um "hash" ou "message digest" dos dados de entrada. É considerado que é

computacionalmente impossível produzir duas mensagens que tenham o mesmo "*message digest*", ou produzir uma mensagem para um "*message digest*" pré-definido.

Com o EAP-MD5, o *Authentication Server* envia um desafio (*challenge*) para o *Supplicant*. O *Supplicant* demonstra que conhece a *password* ao efectuar uma operação de "*hashing*" do desafio e da *password* e enviando o resultado dessa operação para o *Authenticator*.

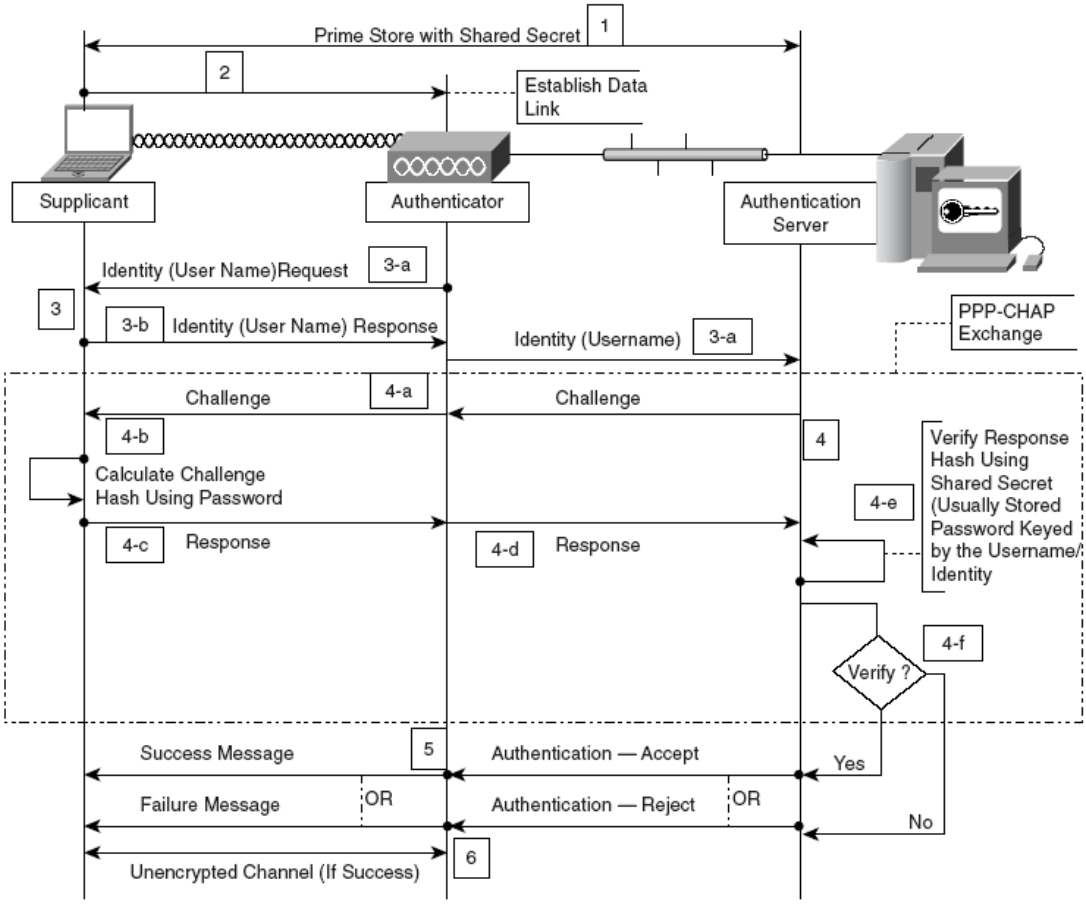

Figura 5-25: EAP-MD5 processo de autenticação [40]

A Figura 5-25 ilustra o processo de autenticação do EAP-MD5. O processo inicia-se com o envio de uma mensagem *RADIUS-Access-Challenge* enviada pelo servidor RADIUS que será empacotada numa mensagem *EAP-Request* pelo *Authenticator* a qual será enviada para o *Supplicant*. O conteúdo *Challenge* é aplicado sobre uma função de "*Hash*" MD5 juntamente com a *password* que o *Supplicant* conhece. O resultado obtido é colocado numa mensagem *EAP-Response* e enviada através do *Authenticator* para o *Authentication Server*. O *Authentication Server* valida a resposta comparando o "*message-digest*" recebido com o valor calculado utilizando o *Challenge* e a password existente na sua base de dados, se os valores forem iguais o *Supplicant* encontra-se validado. É finalmente enviada pelo *Authrntication Server* uma resposta indicando o resultado da operação de autenticação *RADIUS-Access-Accept*

ou *RADIUS-Access-Reject*, que o *Authenticator* transformará em *EAP-Success* ou *EAP-Failure* e reenviará para o *Supplicant*.

Este processo é dos mais fracos em termos de autenticação por duas razões. Não possibilita autenticação mútua (apenas é autenticado o *Supplicant*) e não é criada uma chave de sessão mantendo-se por resolver o problema do tempo de vida das chaves WEP.

5.8.3.2. Lightweight EAP (LEAP)

Este método de autenticação é uma solução proprietária desenvolvida pela Cisco e conhecida por *EAP-Cisco Wireless.* Foi a primeira utilização comercial da norma IEEE 802.1X e EAP em redes sem fios. O modelo básico de funcionamento é semelhante ao WPA, cifrando os dados transmitidos, utilizando chaves WEP geradas dinamicamente, autenticação mútua e suportando mecanismo de *challenge-response*.

O LEAP divide o sistema em três componentes: o *Supplicant*, o *Authenticator* e o *Authentication Server*. O *Supplicant* reside no cliente (STA), o *Authenticator* reside no *Access Point* e o *Authentication Server* é implementado no servidor de RADIUS. O AP necessita de suportar especificamente o protocolo LEAP bem como o IEEE 802.1X. O LEAP utiliza a mesma aproximação no dialogo entre o *Authenticator* e o *Authentication Server* utilizando *EAP over RADIUS.*

O LEAP utiliza mensagens IEEE 802.1X EAPOL, mecanismos de autenticação de servidor e de autenticação de cliente sob a forma de *utilizador/password* através do mecanismo *Microsoft Challenge Handshale Authentication Protocol* (MS-CHAP) em dois sentidos (é enviado um *Challenge pelo Authentication Server* e pelo *Supplicant*).

O processo (Figura 5-26) pode ser sumarizado como se segue:

- O Cliente e o Servidor RADIUS devem partilhar uma palavra-chave secreta, normalmente *username* e *password*.
- Depois de o cliente estabelecer a conectividade inicia o processo de autenticação através do envio de uma mensagem *EAPOL-start* (passo 3), a qual o *Access Point* responde com uma mensagem *EAP-request-identity* utilizando EAPOL (passo 4).
- A resposta do cliente com a sua identificação *EAPOL-response-identity* é enviada para o servidor RADIUS (passo 5).
- A partir deste ponto o AP apenas serve como ponto de passagem até ao passo 7.
- No passo 6 é efectuada a autenticação do cliente através de um mecanismo de pergunta/resposta.

- O *Authentication Server* envia uma *string* aleatória (*Challenge*) para o cliente remoto que pretende acesso.
- O cliente envia uma resposta contendo um "*hash*" que foi produzido utilizando a *password* do utilizador aplicada ao algoritmo LEAP. Entre os dados utilizados encontra-se a *string* (*challenge*) emitida pelo AS.
- O AS calcula também o *"hask*" para comparar com a mensagem recebida do cliente. Se os *Hash* obtidos forem iguais a autenticação teve sucesso. O processo de autenticação do cliente decorreu sem envio de credencias e baseado apenas no conhecimento comum (*password*)

- O passo 7, corresponde à autenticação do servidor através de um mecanismos similar, no fim do qual e caso a autenticação ocorra com sucesso o servidor envia informação sobre as chaves de cifra para o AP que por as enviará para o cliente.
- Tendo sido produzidas e distribuídas as chaves para o cliente e o AP poderá ser iniciado uma comunicação segura.

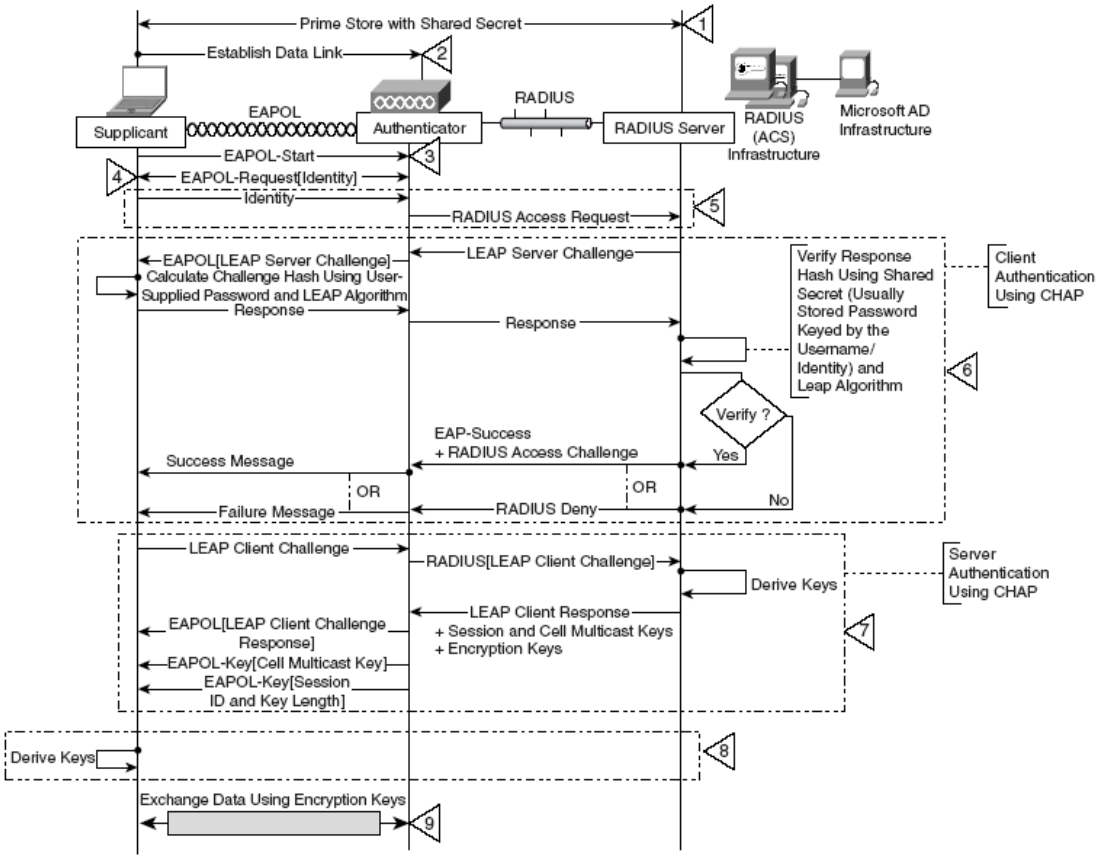

Figura 5-26: LEAP processo de autenticação [40]

O mecanismo de geração de chaves é proprietário e é gerado por cada (re) autenticação, por forma a possibilitar a rotação de chaves. O *timeout* das sessões de RADIUS permite uma rotação periódica de chaves, conseguindo-se assim uma protecção de segurança contra o *sniffing* e o *hacking* das chaves.

5.8.3.3. EAP-Transport Layer Security (EAP-TLS)

O EAP-TLS é um mecanismo de autenticação normalizado pelo IETF (RFC 2716) que é suportado praticamente por todos os fabricantes. Utiliza o protocolo *Transport Layer Security* (RFC 2246) normalizado pelo IETF baseado no protocolo *Secure Socket Layer* (SSL) 3.0 publicado pela Netscape. O EAP-TLS baseia o seu mecanismo de autenticação em certificados digitais X.509 e consequentemente necessita de uma estrutura de suporte PKI. O *Supplicant* tem que possuir um certificado que o *Authentication Server* possa validar, e da mesma forma o *Autentication Server* deverá apresentar um certificado digital ao *Supplicant* para que este o valide. Consegue-se desta forma proporcionar um método de autenticação forte ente o *Supplicant* e o *Authentication Server* (no caso de ambos conseguirem validar os certificados do outro interlocutor).
Depois do processo de autenticação são geradas dinamicamente as chaves WEP (chaves secretas partilhadas) para que o *Supplicant* e o *Authenticator* possam estabelecer uma comunicação segura.

5.8.3.3.1. Introdução ao protocolo TLS

O *Transport Layer Security* (TLS) é um protocolo (Figura 5-27) que permite autenticação e cifra de dados através da criação de um nível entre o TCP/IP e protocolos de rede de níveis superiores como sejam o HTTP.
O TLS é composto por dois layers: O *TLS Record Protocol* e o *TLS Handshake Protocol*. O protocolo *Handshake* envolve a utilização do protocolo *Record* para a troca de uma série de mensagens entre o servidor e o cliente quando estabelece inicialmente a ligação TLS. A troca de mensagens possibilita as seguintes acções:

- Autenticação do servidor perante o cliente.
- Possibilitar ao cliente e ao servidor escolher os algoritmos criptográficos, ou cifras que ambos suportem.
- Opcionalmente autenticar o cliente perante o servidor.
- Utilizar técnicas de cifra com chaves públicas para a geração das chaves secretas.

A troca de mensagens no protocolo *TLS Handshake* envolve os passos descritos de seguida. De notar que o cliente e o servidor trocam entre eles números aleatórios e um numero especial chamado *pré-master secret*. Estes números, juntamente com dados adicionais, permitem a criação de um segredo partilhado por ambos e chamado de *master-secret*. O cliente e o servidor utilizam este *master-secret* para produzir o *Write MAC (Message Authentiucation Code) Secret*, e o *Write Key* (a chave de sessão utilizada para cifra).

1. O cliente envia uma mensagem de "*Client Hello*" para o servidor, que inclui um valor aleatório e o pacote de cifras suportado.
2. O servidor responde enviando uma mensagem "*Server Hello*" para o cliente, incluindo um valor aleatório.
3. O servidor envia o ser certificado para o cliente para que possa ser autenticado e opcionalmente solicita o certificado de cliente. Envia de seguida uma mensagem "*Server Hello Done*"
4. Se o servidor pediu um certificado ao cliente, o cliente envia-o.
5. O cliente cria um "*pré-master secret*", cifra-o utilizando a chave pública obtida no certificado do servidor, e envia-o de seguida para o servidor.
6. O servidor recebe o "*pré-master secret*" e a partir deste, tanto o cliente como o servidor produzem independentemente as mesmas chaves de sessão.
7. O cliente envia uma notificação "*Change cipher spec*" para o servidor indicando que o cliente irá começar a utilizar a utilizar as novas chaves de sessão para *Hashing* e cifra de mensagens.
8. O servidor ao receber a *"Change cipher spec*" e comutar os parâmetros de segurança no "*record layer*" para cifra simétrica utilizando as chaves de sessão. O servidor envia a mensagem "*Server finished*" para o cliente.
9. O cliente e o servidor podem transferir dados entre eles através do canal seguro que estabeleceram. Todas as mensagens trocadas entre o cliente e o servidor são cifradas com as chaves de sessão.

O protocolo TLS Record garante segurança na transferência dos dados das aplicações através da utilização das chaves criadas no protocolo *TLS Handshake*. O protocolo *Record* pela segurança dos dados (cifra), pela verificação de integridade dos dados e validação da origem da mensagem através das seguintes funções:

- Dividir as mensagens para envio em blocos e *assemblar* as mensagens recebidas.

- Comprimir os blocos no envio e descomprimir os recebidos (opcionalmente)
- Aplicar o *Message Authentication Code* (MAC) às mensagens enviadas e verificar a integridade das mensagens recebidos através do MAC.
- Cifrar a mensagens enviadas e decifrar as mensagens recebidas.

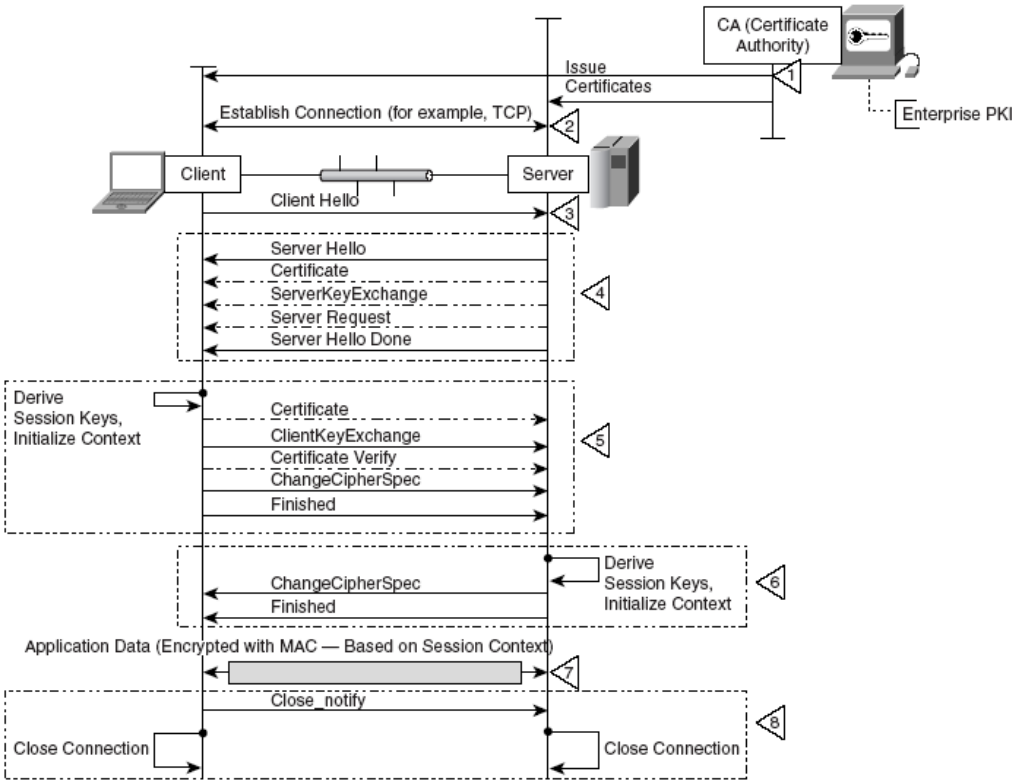

Figura 5-27: TLS processo de autenticação [40]

5.8.3.3.2. Processo de Autenticação EAP-TLS

Tal como já referido as entidades envolvidas no processo de autenticação IEEE802.1X / EAP são: o *Supplicant*, o *Authenticator* e o *Authentication Server*. O *Supplicant* e o *Authentication Server* têm que suportar a autenticação EAP-TLS enquanto o *Access Point* apenas terá que suportar o IEEE 802.1X/EAP.

A Figura 5-28 mostra o processo de autenticação EAP-TLS. O processo de autenticação inicia-se após o envio da mensagem *EAP-Response-Identity* por parte do *Supplicant* através da mensagem *EAP-TLS-Start*. O *Authentication Server* envia o seu certificado juntamente com o pedido de certificado do *Supplicant* na mensagem *EAP-Request*. O *Supplicant* depois de validar o certificado do *Authentication Server* responde com o seu certificado juntamente com a

informação criptográfica suportada. Depois do *Authentication Server* receber a resposta e validar o certificado do *Supplicant* são produzidas as chaves utilizadas para uma criar sessão segura e respondendo ao *Supplicant* e encerrando o processo de negociação de autenticação.

5.8.3.3.3. Geração de chaves WEP com o EAP-TLS

Parte do processo *TLS Handshake* consistiu na geração da chave (*master secret*) possibilitando a criação de um canal seguro entre o *Supplicat* e o *Autentication Server*. Por forma a permitir a criação de um canal seguro (cifrado) entre o *Supplicant* e o *Authenticator*, o *Authenticator Server* envia informação da chaves de sessão para o *Athenticator*. Desta forma, o *Supplicant* e o *Authenticator* podem gerar a chaves WEP necessário à criação de um canal seguro entre eles.

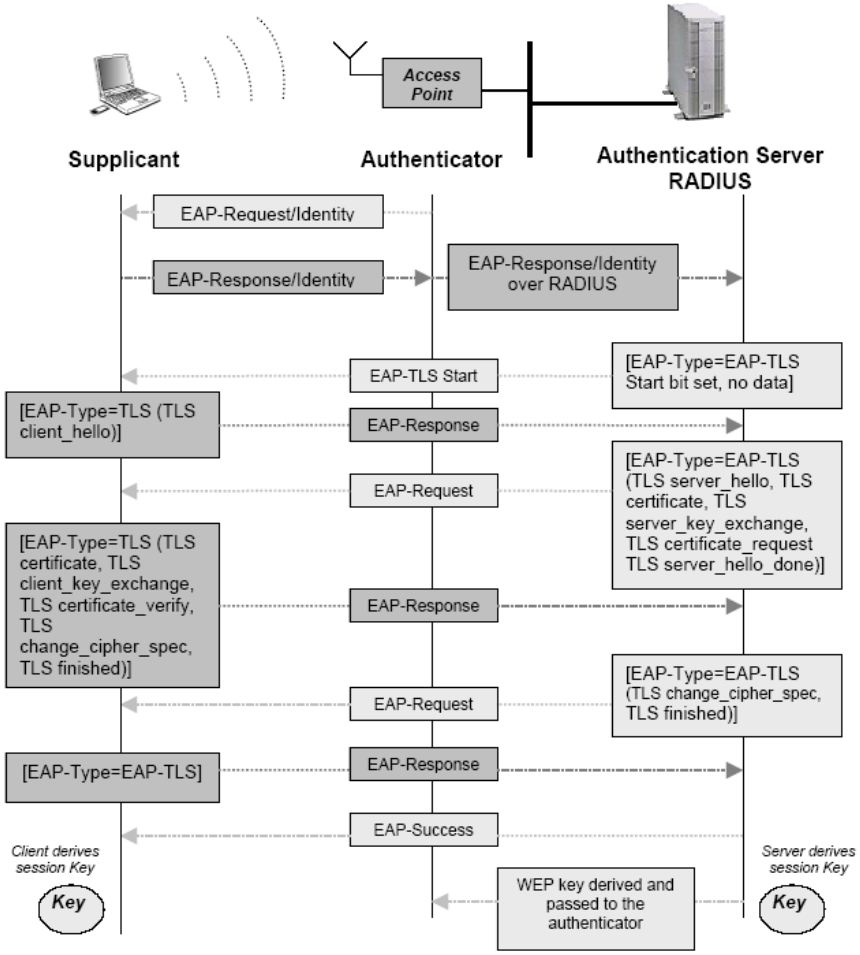

Figura 5-28: EAP-TLS processo de autenticação

5.8.3.4. EAP-Tunneled Transport Layer Security (EAP-TTLS)

O EAP-TTLS (Figura 5-29) é similar ao EAP-TLS, com a diferença que são suportados mais processos de autenticação de cliente depois de ter sido estabelecido um canal de comunicação seguro. O *Supplicant* pode autenticar-se utilizando métodos como sejam *Username/Password*, PAP, CHAP, MSCHAPv2, evitando desta forma a utilização de certificados no *Supplicant*.

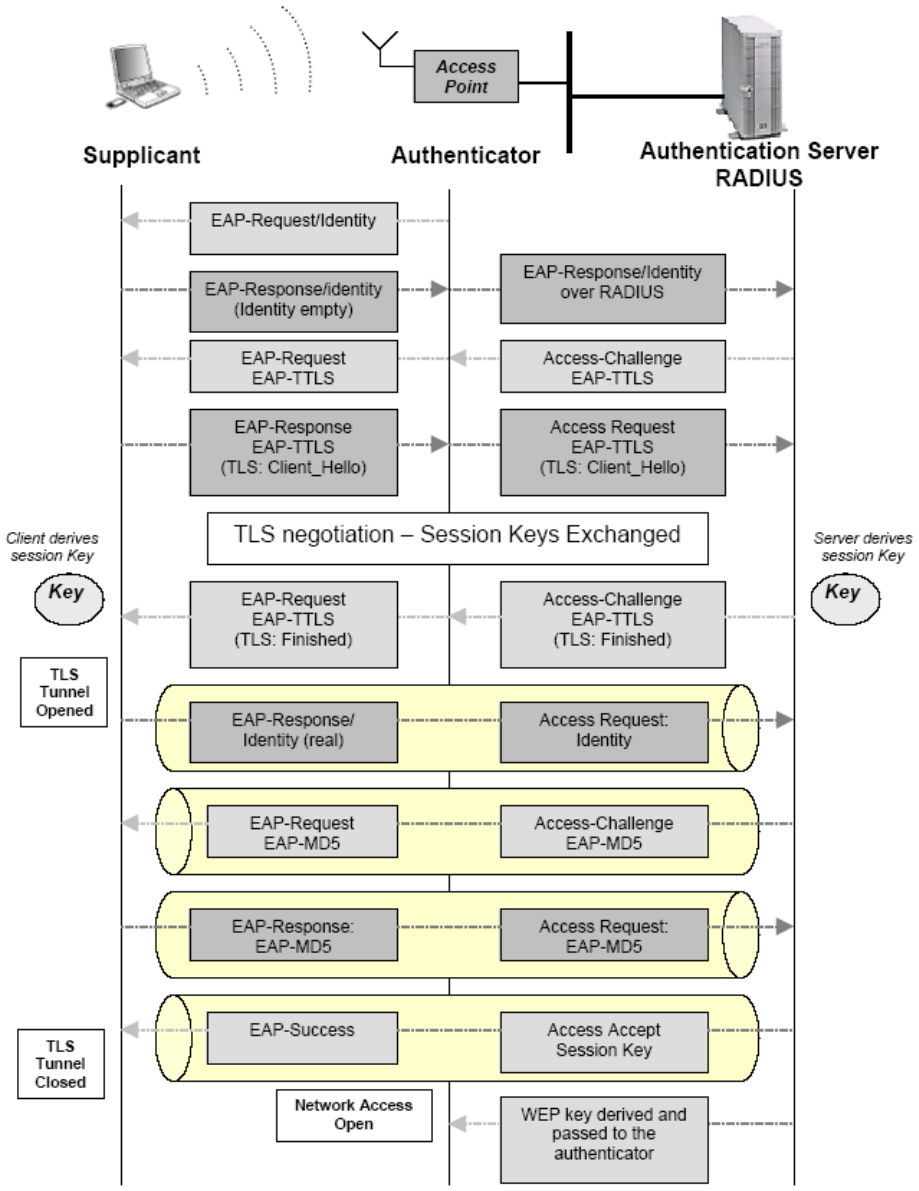

Figura 5-29: EAP-TTLS processo de autenticação

5.8.3.5. Protected EAP (PEAP)

PEAP, tal como o nome sugere, disponibiliza um mecanismo para efectuar de forma segura a negociação EAP. Semelhante ao EAP-TTLS, o PEAP foi desenvolvido em resposta às

dificuldades na implementação de uma estrutura PKI existente no EAP-TLS. A estrutura do EAP-TTLS e do PEAP é similar. Ambos se baseiam em protocolos com duas fases em que na primeira é estabelecido segurança no meio de comunicação e na segunda é efectuado o processo de autenticação. Tal como descrito no caso do EAP-TTLS, a fase 1 estabelece um túnel TLS autenticando o *Authentication Server* perante o cliente através de um certificado. Logo que o canal de comunicação seguro é estabelecido, poderá ser utilizado qualquer outro método EAP para autenticar o utilizador perante o *Authentication Server*. No caso que a autenticação do cliente ser efectuada com sucesso são geradas as chaves de sessão.

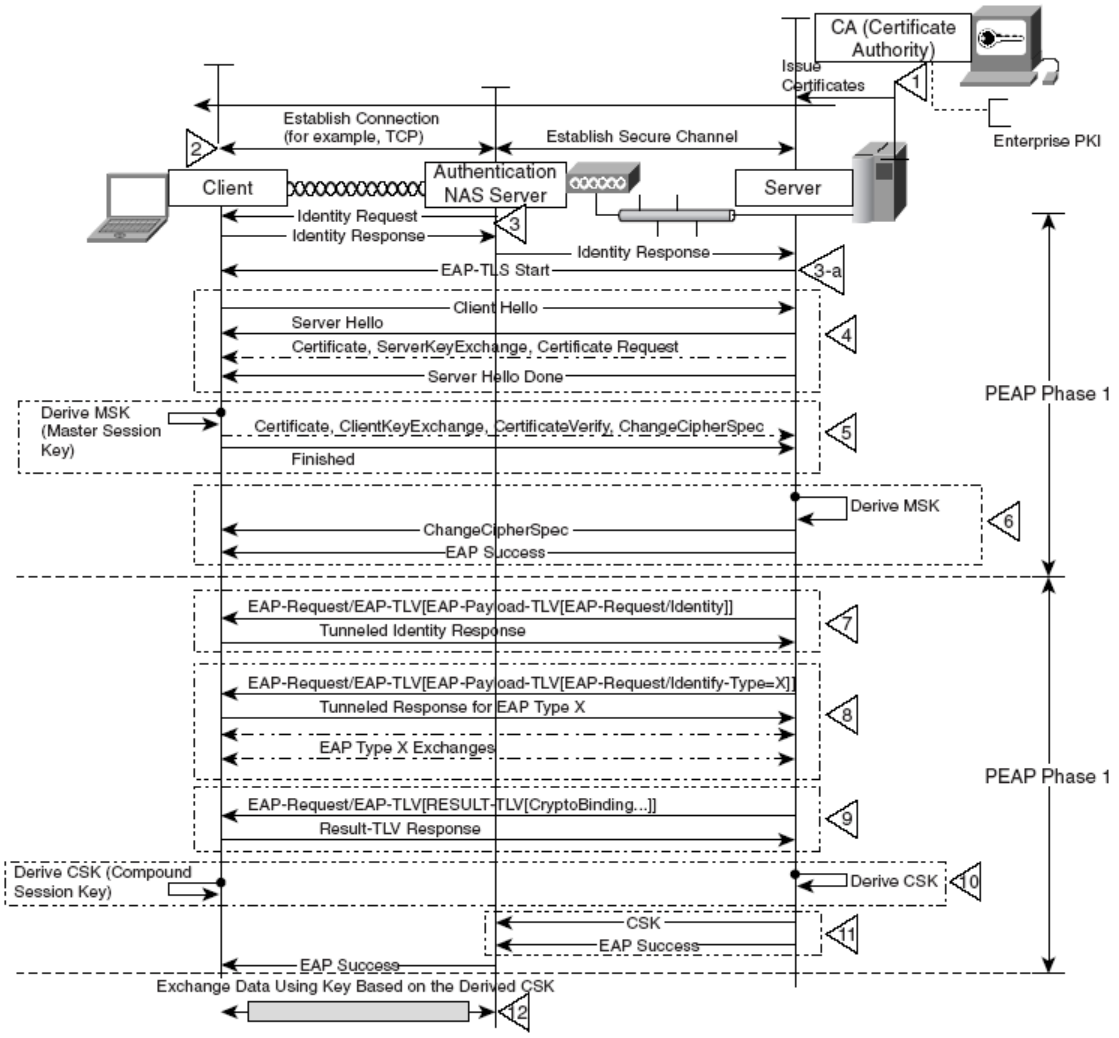

Figura 5-30: PEAP processo de autenticação [40]

A grande diferença entre o PEAP e o EAP-TTLS reside nos métodos de autenticação suportados para autenticação dos clientes depois de estabelecido o túnel seguro. Enquanto o PEAP suporta qualquer método EAP para a autenticação, o EAP-TTLS suporta adicionalmente vários outros

métodos como sejam o *Username/Password*, PAP, CHAP, MS-CHAP, MS-CHAPv2 e SecureID.

5.8.3.6. Comparação dos métodos de autenticação EAP.

A Tabela 5-2 mostra as características principais dos vários métodos EAP apresentados.

Tabela 5-2: Comparação dos protocolos de autenticação do 802.1X

Método	**Descrição**	**Atributos de Autenticação**	**Geração de chaves WEP?**	**Segurança Wireless**	**Dificuldade na Implementação**
MD5	Challenge based Password.	Autenticação num sentido.	Não	Fraca	Fácil
LEAP	Cisco LEAP algorithm (Challenge based password)	Autenticação mútua.	Sim	Melhor que MD5. Mais fraca que outros métodos EAP.	Médio
TLS	Autenticação de Servidor e de Cliente através de certificados.	Autenticação mútua.	Sim	Mais Forte	Difícil
TTLS	Autenticação de Servidor através de certificado. O cliente através de outro método.	Autenticação mútua.	Sim	Forte	Médio
PEAP	Autenticação de Servidor através de certificado. O cliente através de outro método.	Autenticação mútua.	Sim	Forte	Médio

6. Vulnerabilidades e evolução dos controlos de segurança

6.1. Introdução

A segurança constitui um dos aspectos mais importantes em qualquer tipo de redes. Nas redes sem fios este aspecto é essencial, face ao facto do tipo de meio de transmissão utilizado ser um meio partilhado, em que a transmissão de dados é feita por difusão. Os mecanismos de segurança das redes sem fios devem ser robustos de forma a que se consiga implementar as protecções necessárias e suficiente para a informação que a atravessa. A segurança deverá ser obtida através de mecanismos de autenticação (controlo de acessos) e criptografia (protecção dos dados). Na secção 5 apresentou uma descrição dos sistemas de segurança existentes para redes sem fios. De seguida é apresentada uma reflexão crítica a cada um deles.

Desde a publicação da norma IEEE 802.11 que se tem observado uma crescente utilização das redes sem fios, justificada pela mobilidade que permite aos utilizadores e pelos baixos custo de implementação. A primeira forma de introduzir mecanismos de segurança proposta pelo IEEE 802.11 foi a definição do protocolo WEP. Este protocolo tinha como objectivo proporcionar segurança nas redes sem fios e prevenir o risco de uma utilização não autorizada exposta por *access points* inseguros. O protocolo WEP protege o nível "*link*" durante a transmissão entre clientes e *access points* (AP), não proporcionando no entanto uma segurança "*end-to-end*", mas apenas à comunicação entre a estação e o AP. O WEP usa uma cifra contínua RC4 para garantir confidencialidade e um CRC-32 para garantir integridade. As chaves de cifra são simétricas e do conhecimento de ambos os interlocutores, cliente e *access point*, para permitir a troca de tramas. O WEP pode apresentar-se no modo de 64 ou 128 bits, onde são utilizadas respectivamente chaves de 56 e 104 bits de comprimento às quais é concatenado um vector de inicialização (IV) de 24 bits. O protocolo WEP tem inúmeras vulnerabilidades conhecidas resultantes da utilização de chaves estáticas e de um número pequeno de vectores de inicialização que estão descritas na secção 6.2.1.

Para reduzir ou eliminar alguns dos defeitos do WEP, utilizou-se como mecanismo de autenticação o protocolo IEEE 802.1X. Este protocolo é um mecanismo de autenticação baseado em portas, que utiliza métodos baseados em sistemas de chaves públicas ou certificados como seja o EAP-TLS. Estes mecanismos permitem a autenticação mútua entre o cliente e o servidor de autenticação. O IEEE 802.1X apenas define um método robusto para controlo de acessos, não definindo métodos para a protecção dos dados (confidencialidade, integridade) nem para a geração de chaves de cifra por pacote.

O sucessor do WEP foi o *Wi-Fi protected Access* (WPA), introduzido em 2003 pela *Wi-FI Alliance* como um mecanismo intermédio para a substituição do WEP e utilizando um *draft* da norma IEEE802.11i, enquanto esta estava em preparação. O WPA ultrapassa a maioria das vulnerabilidades do WEP através da utilização de chaves dinâmica e temporais, utilizando o protocolo *Temporal Key Integrity Protocol* (TKIP). Este protocolo cifra os dados utilizando cifra continua RC4, com uma chave de 128 bits e um vector de inicialização (IV) de 48 bits.
De modo a ser disponibilizado um mecanismo robusto de segurança para as redes sem fios, o IEEE desenvolveu a norma IEEE 802.11i [37] que apresenta um conjunto de melhorias relativamente ao WEP, nomeadamente a utilização de chaves dinâmicas para cifra de dados, a autenticação 802.1X e a utilização do algoritmo AES para protecção de dados.
O WPA definiu dois modos de operação: o **WPA-PSK** (conhecido por WPA Pessoal) e o WPA-EAP (também conhecido como WPA Empresarial). O primeiro modo baseia-se na utilização de uma chave partilhada (*pre-shared key*) dispensando a utilização do protocolo IEEE 802.1X para autenticação mútua e geração de chaves. As chaves dinâmicas de sessão são derivadas da chave partilhada configurada no cliente e no AP. Este método de operação é muito utilizado em redes sem fios domésticas ou em pequenas empresas.

O **WPA-Empresarial** é utilizado em redes empresariais onde a segurança é um factor crítico para a implementação de redes protegidas. Este modo utiliza o mecanismo de 802.1X para controlo de acesso à rede.
Em resultado da publicação da norma IEEE802.11i a *Wi-FI Alliance* ratificou em Junho de 2004, o *Wi-FI Protected Access 2* (WPA2), como evolução ao WPA. O WPA2 utiliza o algoritmo de cifra *Advanced Encryption Standard* (AES), não tendo actualmente ataques conhecidos. O CCMP é a norma utilizada pelo AES. O CCMP incorpora para garantia de integridade o cálculo do *Message Integrity Check* (MIC) utilizando uma técnica *Cypher Block Chaining* (CBC). As mensagens são cifradas em blocos de 128 bits com uma chave de 128 bits.
O WPA2 também apresenta os mesmos dois modos de operação WAP2-Pessoal (*pre-shared key*) e WPA2-Empresarial (utilizando 802.1X). Estas opções estão todas disponíveis nos actuais sistemas operativos de clientes (Figura 6-1).

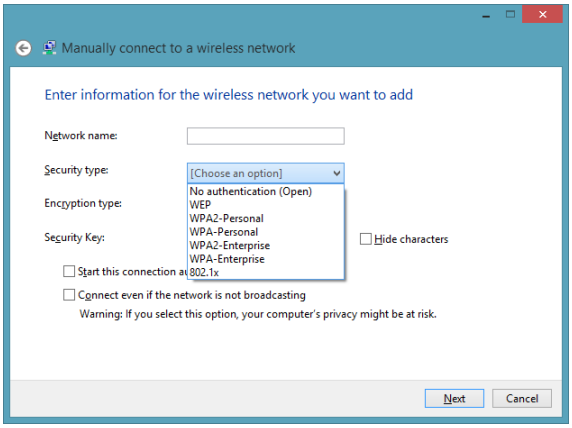

Figura 6-1: Métodos de autenticação WPA, WPA2

6.2. Vulnerabilidades de segurança em redes sem fios

6.2.1. Vulnerabilidades do protocolo WEP

O algoritmo WEP foi definido na norma IEEE 802.11 de forma a proteger as comunicações nas redes sem fios, no entanto logo após a sua publicação apareceram diversos estudos que começaram a mostrar as vulnerabilidades existentes [41] [42] [43].

- **Gestão de Chaves**

A norma IEEE 802.11 não define nenhum mecanismo de gestão de chaves de cifra. A chave partilhada por todos os dispositivos da rede e pelo AP, sendo o processo de alteração efectuado manualmente pelos utilizadores. A distribuição e controlo das actualizações da chave torna-se um processo difícil e moroso e raramente efectuado. A utilização de uma chave estática que não é alterada durante um largo período temporal reduz consideravelmente a segurança.

- **Tamanho da chave estática**

A utilização de chaves de 40 bits é também referenciada como uma fraqueza do WEP, pois permite a utilização de ataques de força bruta.

- **Reutilização de *KeyStream***

A reutilização da sequência de bits (*KeyStream*) proveniente do bloco RC4, e utilizada para cifrar os dados em claro acontece sempre que é utilizada a mesma chave no mesmo dispositivo ou em diferentes dispositivos. Esta situação pode ocorrer em duas situações. A primeira corresponde a uma deficiente implementação do WEP pelos fabricantes através da actualização com pouca frequência do IV (a norma 802.11 recomenda que seja alterado para cada pacote). A

segunda resulta simplesmente do facto de que o IV ter apenas 24 bits de comprimento o que limita o número de chaves possíveis. Se é utilizada uma chave diferente para cada pacote transmitido por cada dispositivo autenticado na rede facilmente observa-se que em poucas horas irão aparecer repetições do IV. Existem alguns métodos publicados para descobrir a *KeyStream* para um dado IV.

- **Algoritmo de *Integrity Check Value* (ICV)**

O WEP ICV é baseado no CRC-32, algoritmo utilizado para detecção de erros de transmissão em redes com fios. O CRC-32 é baseado numa função linear, não sendo considerado como um algoritmo de criptográfico de integridade. Um atacante pode modificar alguns bits da mensagem cifrada e facilmente corrigir o correspondente ICV fazendo parecer ao receptor que está a receber uma mensagem autêntica.

- **Ineficiente utilização do RC4 no WEP**

Foi descoberto [43] que a implementação no WEP do RC4 contém chaves fracas. Ter chaves fracas significa que existe uma correlação entre a chave utilizada e o resultado da *KeyStream*. Descobrir quais pacotes foram cifrados através de uma chave fraca é fácil visto que o IV é transmitido a claro, logo os primeiros três bytes da chave RC4 são conhecidos. É possível deduzir os bytes seguintes da chave através da análise de alguns pacotes (cifrados com chaves fracas).

- **Captura de Mensagens de autenticação**

Tal como descrito no processo de autenticação, através da escuta do meio uma atacante poderá observar as tramas que contêm o "*Challenge Text*" e a resposta que contem a respectiva cifra. Através desta informação é possível obter o KeyStream utilizado para cifrar a resposta e utiliza-lo para outros processos de autenticação futuros.

7. Proposta de metodologia para segurança em redes sem fios

7.1. Proposta de processo de segurança

O desenvolvimento de um processo de segurança (Figura 7-1) que permita uma implementação de segurança nas redes sem fios é fundamental para garantir os requisitos de protecção à informação que circula na rede. A utilização de um *framework* é uma componente chave para sistematizar um processo que permita a identificação, levantamento e gestão dos riscos inerentes à implementação de uma rede sem fios. O processo que se propõe permitirá desenvolver um ciclo contínuo de actividades que possibilitem a identificação dos "desfasamentos" e respectivas iniciativas de melhoria, bem como uma adaptação a alterações dos requisitos ou necessidades de negócio – acesso a informação ou serviços – suportados sobre a rede sem fios.

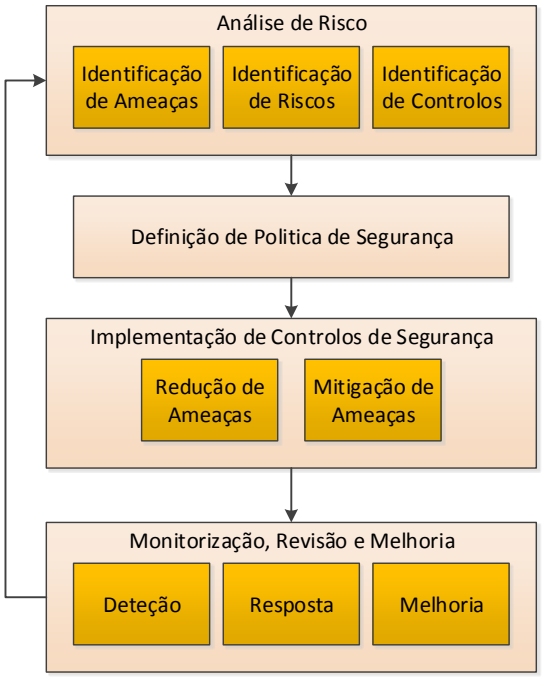

Figura 7-1: Processo de segurança

O processo de segurança será um processo dinâmico e deverá incluir as seguintes fases:

- **Análise de risco**
    - Através do levantamento das necessidades de negócio, objectivos, informação ou sistemas serão desenvolvidas análise de risco que contemplem a identificação de vulnerabilidades e do seu impacto nas vertentes de confidencialidade, integridade e disponibilidade permitindo a identificação e quantificação dos riscos em cada um dos componentes da rede sem fios. Após a

identificação dos riscos serão identificados quais os controlos necessários para a redução dos mesmos a um nível residual aceitável que mitigue as ameaças identificadas.

- **Definição de uma política de segurança para redes sem fios**
    - Definição da visão de segurança relativamente aos requisitos de segurança que devem ser contemplados na implementação da rede sem fios e que visem os controlos identificados na fase anterior, através de definição dos mecanismos e serviços de segurança;
- **Implementação de controlos de segurança**
    - Em face da identificação dos controlos e mecanismos de segurança identificados, procede-se à sua implementação;
- **Monitorização, revisão e melhoria**
    - A detecção de falhas de segurança nas redes sem fios, em resultado de incidentes reportados ou de avaliações de segurança, deverá ser inserida num plano de resposta a incidentes e contemplar a identificação de melhorias que irão ser analisadas no próximo ciclo do processo.

Com esta proposta de *framework* pretende-se desenvolver um processo continuo que apoie as empresas na criação e manutenção do nível de segurança necessário para a protecção da informação e recursos nas redes sem fios.

Descreve-se nas secções seguintes as diversas fases do processo.

7.2. Análise de risco

O Conceito de Segurança descrito neste documento baseia-se no processo de gestão de risco da ISO 27005 [7] (Figura 7-2).
O processo de gestão de risco tem os seguintes passos:

- **Estabelecimento de contexto** – Destina-se a identificar e delimitar o âmbito e os limites da avaliação;
- **Avaliação de Risco** – esta fase é efectuada através de duas componentes:
    - Identificação dos riscos – com a enumeração dos activos, ameaças e vulnerabilidades
    - Estimativa de risco – em que os riscos são quantificados e prioritizados;

- **Tratamento de Riscos** – processo de identificação, selecção e implementação de medidas de segurança para cada um dos riscos identificados; As medidas de tratamento de riscos podem incluir a inibição, transferência ou contenção de riscos. Estas medidas podem ser seleccionadas de conjuntos de medidas de segurança já em vigor no seio da Organização como sejam as Descrições de funções de segurança implementadas tecnicamente e procedimentos estabelecidos ou novas medidas de segurança.
- **Aceitação de Riscos** – é o processo em que riscos residuais, que não foram mitigados pelas medidas de tratamento de risco identificadas, são assumidos pela organização. Estes riscos residuais, uma vez aceites, formam um conjunto de riscos que, face à avaliação efectuada com base no seu nível e extensão, são conscientemente assumidos como comportados pela gestão da Organização.

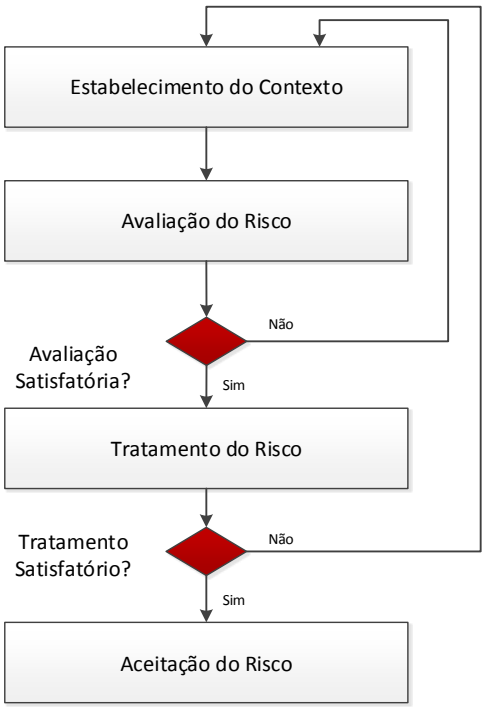

Figura 7-2: ISO 27005 - processo de gestão de risco

7.2.1. Estabelecimento do contexto

Nesta fase do processo devem ser identificados os objectivos e necessidades de negócios e prioridades e prioridades tendo em vista identificar e delimitar o âmbito e os limites da avaliação. Devem também ser definidos os critérios de avaliação de riscos que estarão presentes no ciclo de vida que o processo terá.

7.2.1.1. Identificação de critérios

Para a identificação dos critérios de avaliação de riscos devem ser considerados os seguintes factores:

- O valor estratégico para o processo de negócio.
- A criticidade dos activos de informação envolvidos.
- Requisitos legais, regulamentares ou contratuais.
- Importância para o negócio nas vertentes de disponibilidade, confidencialidade e integridade.
- Expectativas dos *Stakeholders*
- Reputação

Desta forma identificam-se os seguintes tipos de critérios que é necessário definir:

- Critérios de impacto - Os critérios devem ser desenvolvidos e especificados em termos do escalão de danos ou custos para a organização:
    - Nível de classificação do activo de informação que foi afectado
    - Quebras na segurança da informação (perda de confidencialidade, integridade e disponibilidade)
    - Perdas financeiras ou de negócio
    - Disrupção de planos ou compromissos
    - Danos na reputação
    - Quebras nos requisitos legais, regulamentares ou contratuais
- Critérios de aceitação - Este critérios dependem normalmente das políticas da organização, objectivos, metas, e interesse dos *stakeholders*. Cada organização deve desenvolver a sua escala para níveis de aceitação de risco:
    - Critério deve incluir múltiplos indicadores com limites que ajudem a gestão a aceitar o risco em determinadas condições.
    - Critério de aceitação pode ser expresso como uma relação entre um benefício de negócio (ex: lucros) e o risco estimado.
    - Diferentes critérios de aceitação podem ser aplicados a diferentes classes de risco.
        - Ex: Riscos que comprometam aspectos legais podem não ser aceites, mas riscos elevados podem ser aceites se estiver especificado contratualmente.

- Critérios de aceitação podem conter requisitos para actividades adicionais futuras.
    - (ex: aceita-se o risco se a acção de redução de risco for implementada num determinado tempo)

7.2.1.2. Âmbito e fronteiras

Deve ser definido o âmbito e as fronteiras para o processo de gestão de risco. O âmbito é necessário para garantir que todos os Activos relevantes são levados em conta no levantamento dos riscos. As fronteiras são necessárias para se identificarem os riscos que as podem atravessar. Informação da organização deverá ser recolhida para determinar o ambiente onde opera e a sua relevância para o processo de Gestão de Risco.
Informação a considerar:

- Objectivos estratégicos de negócio, estratégias e políticas
- Processos de negócio
- A estrutura e funções na organização
- Requisitos legais, regulamentares ou contratuais.
- A política de segurança da informação
- A aproximação geral à gestão de risco
- Activos de informação
- Localização e características geográficas da organização
- Expectativas dos *stakeholders*
- Ambiente sociocultural

Especificamente no âmbito de uma rede sem fios deverão ser recolhidos, entre outras, as seguintes informações:

- Identificação das instalações onde é necessário implementar a rede, por forma a ser desenvolvido um *site survey*, e o dimensionamento da rede e suas características;
- Identificar ou utilizadores ou os grupos de utilizadores que necessitam de ter acesso através da rede;
- Identificar os recursos, aplicações ou sistemas, que os utilizadores ou grupos de utilizadores necessitam acesso, por forma a identificar perfis de acesso;
- Identificar a informação de negócio, aplicações ou serviços que ficaram acessíveis desde a rede sem fios;

7.2.1.3. Organização para processo de gestão de risco

Deve ser definida a estrutura organizacional e responsabilidades pelo processo de gestão de risco, para que seja garantido o ciclo de vida dos processos de segurança.

Principais papéis e responsabilidades:

- Desenvolvimento de um processo de gestão de risco adequado para a organização.
- Identificação e análise dos *stakeholders*.
- Definição dos papéis e responsabilidades de todas as partes tanto internas como externas à organização.
- Estabelecimento das relações necessárias entre a organização e os *stakeholders,* bem como interface com as funções de gestão de topo, ou outros projectos relevantes.
- Definição do caminho de escalonamento de decisões.
- Especificação dos registos que devem ser mantidos.
- Esta organização deverá ser aprovada pelos gestores de topo.

7.2.2. Avaliação de risco

Processo formal de identificar, quantificar ou descrever qualitativamente e priorizar riscos na organização. Procura identificar os riscos que podem numa organização comprometer a capacidade de cumprir as responsabilidades por indisponibilidade de alguma das suas componentes físicas, tecnológicas, organizacionais ou documentais.

Tem como informação de base:

- Informação obtida na fase de Estabelecimento de Contexto

Produz no fim desta fase:

- Lista de riscos ordenada por prioridades.

Aspectos importantes:

- Liderança forte e com apoio ao mais alto nível
    - Como resultado do levantamento poderá ser necessário implementar controlos, com impacto directo em orçamentos.
- *Stakeholders* com conhecimentos e responsabilidade

7.2.2.1. Identificação dos riscos

A identificação do risco visa determinar quais os riscos existentes ou previstos, no contexto definido, quais são as suas características, qual a sua duração e resultados possíveis.

A estimativa do risco adopta uma metodologia qualitativa ou quantitativa, utilizando uma escala de cinco níveis - **muito baixo, baixo, médio, alto e muito alto** - e é expressa em termos de:

- **Probabilidade** - A probabilidade de ocorrência de um risco identificado. Vários factores afectam a probabilidade, tais como:
    - O esforço necessário para desencadear um ataque;
    - Os benefícios obtidos com um ataque bem-sucedido;
    - As motivações (ego, espionagem, vingança, fanatismo, terrorismo, etc.);
    - O risco de ser detectado;
    - Vulnerabilidades exploráveis;
    - O número potencial de atacantes.
- **Impacto** - A quantidade de valor que um activo (ou conjunto de activos) em termos de perdas (quantitativas ou qualitativas) se for alvo de um ataque bem-sucedido. Os impactos podem ser de diversas naturezas, a saber:
    - Financeiro;
    - De reputação;
    - Operacional;
    - Legais e regulamentares.

7.2.2.2. Identificação dos activos

Esta fase inicia-se com a identificação dos riscos através da identificação dos activos (*assets*) dentro do âmbito e fronteiras definidos previamente através de um processo de que contempla:

- **Planificação de actividades de análise de risco** - A condução de uma análise de risco, pode ser um processo complicado, que requer um investimento temporal significativo de diversos participantes (*stakeholders*) envolvidos nos processos de negócio.
    - Alinhamento: ao nível orçamental, grupo de segurança como parceiro proactivo;
    - Âmbito: deverá documentar todas as funções da organização na análise de risco;
    - Aceitação dos *stakeholder*s: assegurar que compreendem a importância da avaliação de risco, convidando-os a uma participação activa.
    - Definir expectativas razoáveis: o processo requer muitos contributos de diferentes grupos que possivelmente representam toda a organização.

- Ao serem levantados os processos de negócio, aplicações, sistemas recursos, instalações dentro do âmbito, são também identificadas as unidades de negócio que participam.

- **Recolha de Informação** - de acordo com o planeamento são efectuadas várias interacções com elementos da organização (*stakeholders*) para a identificação e **levantamento** de riscos associados a activos que estejam dentro do âmbito do processo em análise:
  - **Activos** da Organização
    - Tudo o que tem valor para a organização e que requer protecção
    - Descrição de cada Activo
    - Pequena descrição do Activo, o seu valor e o seu responsável (*owner*) e processos de negócio onde participa.
  - **Ameaças**
    - Causas ou acontecimentos que podem afectar negativamente um Activo, nas vertentes de disponibilidade, integridade e perda de confidencialidade.
  - **Vulnerabilidades**
    - Fraquezas ou falta de controlos que possam ser utilizados para afectar um Activo.
  - **Controlos actuais**
    - Descrição dos controlos actuais e da sua eficácia
  - **Controlos propostos**
    - Ideias iniciais para redução de riscos
  - **Participantes nesta fase:**
    - Irão ser efectuados contactos com diferentes grupos e intervenientes pelo que deverá ser levantada a função de cada um nos processos bem como a sua área de actuação.

O resultado desta actividade será uma **Lista de Activos** a ser analisados e processos de negócio associados.

7.2.2.3. Identificação das ameaças

Na fase de recolha de informação segue-se a identificação de ameaças:

- Recolha de Informação / **Ameaça**

- **A causa de um potencial impacto na organização** - danificar um Activo como sejam Informação, processos e sistemas. Podem ter origem humana ou natural e serem acidentais ou deliberadas.
- Devem ser identificadas genericamente e por tipo (ex: acções não autorizadas, danos físicos, falhas técnicas), não devendo ser esquecida nenhum ameaça (mesmo uma não esperada).
- Algumas ameaças podem afectar mais que um Activo, causando por isso diferentes impactos.
- **Fontes de Informação:**
  - As ameaças às empresas podem ser identificadas através da produção de cenários, pela criação de listas de tipificação, pela revisão de incidentes, pela informação dos responsáveis dos Activos/Bens, ou outras fontes.
  - Ver exemplo ISO 27005/Anexo C ou outra fonte de informação relativa a ameaças em redes sem fios.
  - Auditorias de segurança às plataformas em actividade.
  - Resultados de "*Site Survey*" de Radiofrequência das instalações.
  - As tabelas de ameaças devem ser mantidas actualizadas (mudanças ambientais, infra-estruturas tecnológicas, mudanças de legislação, etc.)

O resultado desta actividade será uma **Lista de Ameaças** associadas a cada activo.

7.2.2.4. Identificação dos controlos existentes

A actividade seguinte na fase de recolha de informação consiste na identificação de controlos existentes.

- Recolha de Informação / **Identificação de Controlos Existentes**
  - A identificação de controlos existentes permite evitar investimentos ou trabalho desnecessário em caso de duplicação de controlos.
  - Enquanto se identificam os controlos também se deve verificar se estão a funcionar correctamente.
    - Se não funcionarem correctamente podem causar vulnerabilidades.
  - Podem equacionar-se situações onde controlos não funcionem, podendo ser necessário novos controlos (melhorias) para endereçar os riscos identificados.

- Para estimar o efeito de um controlo deveremos avaliar quanto ele reduz a probabilidade da ameaça explorar a vulnerabilidade, ou reduz o impacto no incidente.

O resultado desta actividade será uma **Lista de de controlos existente** para cada activo, seus estados de funcionamento e associações às ameaças/vulnerabilidades.

7.2.2.5. Identificação do nível de exposição ao risco

A actividade seguinte na fase de recolha de informação consiste na identificação do nível de exposição ao risco.

- Recolha de Informação / **Identificação o Nível de Exposição**
  - **Identificação da exposição ao risco** para cada combinação de Ameaça / Vulnerabilidade identificada
  - Utilizam-se normalmente três níveis: **Alto, Médio e Baixo**
    - Exemplo: Num activo digital classifica-se a exposição alta se uma vulnerabilidade permite um controlo administrativo ou de "*root*".

O resultado desta actividade será a **identificação do nível de exposição para cada risco** associado aos activos.

7.2.2.6. Estimação do nível de risco – Impacto

A actividade seguinte tem o objectivo de identificar o impacto associado ao risco quando uma ameaça explora uma vulnerabilidade, em face dos aspectos referenciados na secção 7.2.1.1.

- Avaliação das consequências / **Impacto**
  - **Valorização dos Activos:**
    - **Quantitativa** (ALE - valor que se vai perder num ano se o risco não for atenuado) *Annual Loss Expectancy*:
      - Valor de substituição de Activo (ou parte)
      - Custo de recuperar com novo activo com recuperação da informação (se possível).

- Consequências da perda ou comprometimento do Activo
- Financeiras, legais, etc.

- **Qualitativa**
  - Em função dos estragos potencias, provocados pelas ameaças na exploração de vulnerabilidades são definidas Classes de Exposição sobre várias vertentes:
  - Vantagens competitivas, legal, reputação, etc.

As consequências podem ser expressas em termos monetários, técnicos ou **critérios de impacto (**Tabela 7-1**)**.

Tabela 7-1: Tabela de impactos (exemplificativa)

Score	Tipo de impacto	Impacto financeiro	Impacto não financeiro
1	Insignificante **Impacto insignificante para o negócio**	Menor que 50.000 €	Impacto insignificante para o negócio Acesso a redes públicas ou informação pública.
2	Baixo **Impacto baixo nos processos críticos**	50.000 € até 500.000 €	Impacto baixo em processos críticos Acesso a informação de uso interno. Indisponibilização de uma rede de dados departamental (<5% utilizadores).
3	Médio **Impacto significativo nos processos críticos**	500.000 € até 5.000.000 €	Impacto significativo nos processos críticos Acesso a informação classificada da organização. Perturbação na disponibilização dos recursos de rede ou aplicações de negócio (até 50% dos utilizadores).
4	Alto **Impacto severo nos processos críticos**	5.000.000 € até 15.000.000 €	Impacto severo em processos críticos. Acesso a informação confidencial ou secreta. Perturbação na disponibilização dos recursos de rede ou aplicações de negócio (entre 50% e 75% dos utilizadores).
5	Catastrófico **Sobrevivência do negócio ameaçada**	Maior que 15.000.000 €	Sobrevivência da Instituição ameaçada Perturbação na disponibilização dos recursos de rede ou aplicações de negócio (em >75% dos utilizadores).

Outra abordagem para a determinação do índice de impacto, levando em conta os factores de confidencialidade, integridade e disponibilidade, poderá ser efectuada através da utilização de uma relação:

Impacto = MAX (Ind_Confidencialidade, Ind_Integgridade, Ind_Disponibilidade)

Cada um dos índices terá definido uma escala de 5 níveis, que refletem o efeito que uma determinada ameaça tem sobre ele (ex: Tabela 7-2: Tabela de impacto na confidencialidade).

Tabela 7-2: Tabela de impacto na confidencialidade

Nível Confidencialidade	Valor	Descrição
Baixo	1	Informação em claro ou pública.
Médio	2	Acesso a informação de uso interno na organização.
Alto	3	Acesso restrito numa base de necessidade de saber, dentro de grupos ou equipas (ex: contractos)
Muito Alto	4	Restrito a um individuo ou grupo limitado (ex: notícias criticas, planos de negócio, etc), o acesso não autorizado pode causar danos elevados.

O resultado desta actividade será a **identificação do impacto para cada risco/ameaça** associado ao activo.

7.2.2.7. Estimativa do nível de risco – Probabilidade

Face a cada risco identificado será necessário **avaliar a probabilidade** de o mesmo ocorrer em face dos aspectos referenciados na secção 7.2.1.1.

- Avaliação das consequências / **Probabilidade**
    - Em função de informações estatísticas, como sejam o histórico de incidentes de segurança, ou fontes de informação externas, será identificada a **probabilidade** de um determinado risco ocorrer.
    - Utilização de métricas definidas pela organização:
        - **Muito Alto –** um ou mais impactos são esperados num mês
        - **Alta** – um ou mais impactos são esperados num ano
        - **Médio** – expectável ocorrer entre dois e três anos
        - **Baixo** – não é expectável que ocorra nos próximos 3 anos
        - **Muito baixo -** não é expectável que ocorra.

O resultado desta actividade será a **identificação da probabilidade para cada risco/ameaça** associado ao activo.

7.2.2.8. Estimativa do nível de risco – Cálculo do risco

A estimativa do nível de risco será calculada em função dos valores de probabilidade e impacto calculados nas fases anteriores. Este quantificador poderá assumir uma escala de cinco níveis - **muito baixo, baixo, médio, alto e muito alto**, sendo o seu cálculo obtido através de uma matriz de risco (Tabela 7-3) definida.

Tabela 7-3: Matriz de risco

Impacto **Probabilidade**	**1**	**2**	**3**	**4**	**5**
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	40	25

Para cada risco identificado na tabela de risco (Tabela 7-4) é efectuado o cálculo e preenchido o nível de exposição ao risco.

Tabela 7-4: Tabela de riscos (exemplo)

	Recursos Afectados			**Índice de Risco**			
Risco	Pessoas	Instalações	Sistemas	Impacto	Probabilidade	**Exposição ao Risco**	Racional
Negação de Serviços (DoS)	v	v	v	Muito Elevado	Baixa	**Média**	Empastelamento do sinal de Radiofrequência.
Intercepção de comunicações			v	Muito Elevado	Media	**Alta**	Escuta do meio de Radiofrequência

O resultado desta actividade será a uma **Lista de riscos** associados a cada activo.

7.2.3. Tratamento do risco

Tendo sido efectuada a identificação de todos os riscos dentro do âmbito definido, passa-se agora à fase de tratamentos dos riscos. Para cada risco são identificadas as medidas que possam modificar o risco. A implementação das medidas (ou controlos) identificadas irá modificar o nível de exposição do risco.

O tratamento do risco implica um processo cíclico que inclui:

- Apreciar um tratamento do risco;
- Decidir se os riscos residuais são toleráveis;
- Se não forem toleráveis, gerar novo tratamento de risco;
- Apreciar a eficácia desse tratamento.

Existem quatro estratégias de lidar com os riscos:

- **Reduzir o risco** - O nível de risco deve ser reduzido através da selecção de controlos de forma que o risco residual possa ser considerado aceitável, como sejam:
  - Eliminar a fonte do risco
  - Alterar a sua probabilidade
  - Alterar o seu impacto
- **Evitar o risco -** Identificar actividades ou condições que permitem que determinado risco possa ser evitado, podendo ser decidido parar ou não iniciar actividades;
- **Transferir o risco -** O risco pode ser partilhado ou transferido para outra(s) entidade(s) (incluindo contratos ou financiamento de risco).
- **Aceitar o risco** de forma informada
  - Assumir o risco não efectuando nenhuma acção.
  - Assumir o risco (ou mesmo aumentando) para obter uma oportunidade.

A selecção da opção de tratamento do risco mais apropriada implica comparar os custos e os esforços da sua implementação com os benefícios resultantes, tendo em conta os requisitos legais, regulamentares.

O resultado desta actividade será **um plano de tratamento dos riscos** com a estratégia de tratamento para cada um dos riscos identificados na Lista de Riscos associados a cada activo.

O plano de tratamento dos riscos (Tabela 7-5) deverá claramente identificar a ordem de implementação dos tratamentos individuais do risco. Este plano tem como objectivo

documentar a forma como as opções de tratamento escolhidas serão implementadas. A informação fornecida nos planos de tratamento deverá incluir pelo menos:

- Razões para a selecção das opções de tratamento, incluindo benefícios esperados
- As acções propostas
- Os requisitos de recursos, incluindo contingências
- A calendarização e o cronograma

Tabela 7-5: Plano de tratamento de riscos

Risco	Descrição do risco	Tipo de risco	Detentor do risco	Classificação / Prioridade	Situação do projecto	Comentários
Captura de informação na rede	Os mecanismos criptográficos utilizados na ligação da rede sem fios são fracos.	Segurança	Responsável de Segurança	Alta	Não Iniciado	Identificados equipamentos a subsistir. Espera-se aprovação para adjudicação
Rouge APs	Existência de AP com os mesmos SSID nas instalações.	Segurança	Responsável de Segurança	Médio	Iniciado	Identificados e adquiridos os WIDS. Em fase de instalação

7.2.4. Aceitação do risco

Os riscos residuais, que não foram mitigados pelos controlos (medidas de tratamento de risco) identificados, deverão ser assumidos pela organização. Estes riscos residuais, uma vez aceites, formam um conjunto de riscos que, face à avaliação efectuada com base no seu nível e extensão, são conscientemente assumidos como comportados pela gestão da Organização.

7.3. Definição de política de segurança de rede sem fios

Estando terminada a fase de avaliação de risco descrita nas seções anteriores, e seguindo a metodologia proposta, torna-se necessário definir a política de segurança e um plano de implementação de controlos que vise mitigar os riscos identificados em face da prioridade definida.

7.3.1. Política de segurança de rede sem fios

A política de segurança para as redes sem fios tem como objectivo definir a postura da entidade face à segurança a implementar para a protecção dos activos, tendo em conta os riscos identificados e o nível de risco residual definido. Nesta política devem ser expressas as responsabilidades pela gestão das redes e dos dispositivos envolvidos na implementação de

redes sem fios (ex: AP, servidores RADIUS, dispositivos de clientes, etc), as condições para a colocação dos dispositivos de rede, os protocolos de segurança permitidos, os perfis de utilizadores e suas condições de acesso.

Neste documento deve ser identificado o âmbito e fronteiras de responsabilidade e deverá reflectir, entre outros, os seguintes pontos:

- Dispositivos de rede sem fios autorizados
    - Quais os APs permitidos e suas configurações de segurança obrigatórias;
    - Protocolos autorizados de autenticação e de cifra.
    - Responsabilidades de gestão dos dispositivos de rede;
    - Monitorização do espaço RF, dos dispositivos de rede, de acessos não autorizados e notificação de incidentes;
    - Instalação de APs em DMZ com regras de controlo de fluxo especificas em função de perfis de acesso (ex: SSID),
- Dispositivos de acesso autorizados
    - Todos os dispositivos com rede sem fios, como sejam computadores portáteis, smartphones, PDAs e tablets;
    - As condições de acesso dos dispositivos (Sistemas operativos, protocolos de segurança WPA/WPA2, certificados, etc), podendo ser diferenciadas em função do mesmo pertencer à entidade que fornece a rede ou a um estranho à mesma.
- Perfis de utilizadores e serviços autorizados
    - Deverão estar especificados os perfis de utilizadores autorizados e os seus acessos;
    - Devem estar especificados os serviços e aplicações a disponibilizar através da rede sem fios e suas condições de acesso. Estes recursos poderão ser agrupados de forma a permitir uma gestão baseada em perfis (que se poderá traduzir por exemplo na implementação de diversos SSID em função da criticidade dos recursos a aceder);
    - Quem autoriza o acesso aos utilizadores;
    - Regras de acesso e utilização da rede sem fios e respectivos recursos;
    - Regras para o utilizador proteger o seu dispositivo;
- Controlo de acessos
    - Método de acesso à rede (palavras chave, certificados, tokens, etc);
    - Acesso aos recursos em função do tipo de autenticação e em função do perfil de acesso do utilizador.

O documento de política deverá ser aprovado, publicado e do conhecimento de todos os utilizadores que utilizem a plataforma de redes sem fios.

7.3.2. Plano de implementação de controlos

Estando identificados os requisitos de segurança obrigatórios, vertidos na Politica de Segurança da rede sem fios e desenvolvida a análise de risco, torna-se possível desenvolver um plano de implementação dos controlos a aplicar na rede sem fios.
Para os controlos identificados na análise de risco, torna-se necessário escolher as estratégias e soluções de implementação. Apresentam-se na Tabela 7-6 algumas das estratégias propostas para implementação.
Em função do estado de desenvolvimento da entidade (primeira implementação ou actualização de controlos) o plano de implementação deverá reflectir a implementação dos controlos identificados no Plano de Tratamento dos Riscos resultado da Análise de Risco.

Para uma implementação inicial de uma rede sem fios, deveremos incluir no plano as seguintes actividades:

- Desenvolver a política de segurança para rede sem fios;
- Desenvolver e implementar políticas de palavras-chave fortes, mecanismos de autenticação forte (tokens, certificados, etc);
- Sensibilizar os utilizadores sobre riscos e segurança nas redes sem fios;
- Promover a instalação de *hardware/software* certificado para utilização de WPA/WPA2.
- Efectuar um levantamento RF (*site survey*) em todas as instalações da entidade, permitindo obter informação para o desenho da melhor distribuição de AP em fase de concepção, e possibilitando também identificar possíveis tentativas de ataque (*rouge APs*);
- Desenvolver uma arquitectura física e lógica para a implementação de rede sem fios;
- Estabelecer um processo validado em termos de rede e segurança para a implementação de dispositivos de rede sem fios (AP);
- Definir as regras de implementação de dispositivos de rede (áreas físicas, interior ou exterior de edifícios);

Tabela 7-6: Estratégias de implementação de controlos

Controlo	Métodos de Implementação
Desenvolvimento de política de rede sem fios	Em face do levantamento das necessidades de acesso do utilizadores e da criticidade dos recursos ou informação a aceder é necessário ter definida uma política de segurança que especifique as regras e responsabilidades.
Segregação da rede em SSIDs	Em função das diferentes necessidades de acesso aos recursos poderá ser definida uma arquitectura de rede com diferentes SSID que permita implementar regras de segurança de acesso distintas. Como exemplo poderá existir um SSID para convidados com acesso único à internet em função de uma credencial fornecida numa base temporal
Implementação de controlos de acesso diferenciado	Poderão ser utilizados diferentes métodos de autenticação que permitam de base a decisão de acesso recursos de rede. Cada SSID disponibilizado poderá ter associado um requisito de método de autenticação que lhe permitirá acesso a recursos com níveis de segurança distintos. A escolha de mecanismos como seja WEP, 802.1X, PSK, controlo de acesso por MAC poderão servir para acesso a redes de perfil de segurança baixo. Para uma utilização profissional deverão se utilizados mecanismos que permitem autenticação forte, que utilizando certificados, tokens de *hardware/software* e protocolos como sejam WPA2 empresarial com EAP-TLS integrado com uma Active Directory (através de serviço Radius) para utilização das credenciais de domnio.
Cifra de dados nas redes sem fios	Como toda a informação que circula na rede sem fios é passível de ser escutada´, torna-se necessário escolher os protocolos de cifra seguros. A utilização preferencial de WPA2, que utiliza o protocolo AES é a resposta adequada.
Protecção forte nos dispositivos de rede	Os equipamentos AP e outros dispositivos de redes poderão ficar expostos a ataques, pelo que deverá ser implementada uma política de configuração de segurança robusta (hardening). Para além destes equipamentos deverão também ser objecto de um reforço de segurança todos os dispositivos da arquitectura de rede sem fios (firewall, routers, switchs, etc).
Protecção a cliente das redes sem fios	A configuração dos equipamentos cliente deverá cumprir os requisitos necessários para garantir um correto acesso e utilização dos recursos da rede. Estas configurações poderão ser imposta e aplicadas automaticamente (exemplo na utilização de Windows Group Policy Objects para configuração dos parâmetros de WLAN do posto/utilizador).
Monitorização do tráfego de rede de fios	A descoberta de dispositivos *wireless* não autorizados poderá ser efectuada através de monitorização do especto FR. A utilização de sistemas *wireless intrusion ou prevention systems* (WIDS/WIPS) permitem a monitorização em tempo real e a notificação de ataques ou violações de segurança.

Reforço da segurança da rede	Os desafios para a arquitectura de rede empresarial perante introdução de redes sem fios numa organização poderão ter implicações e obrigar a repensar o desenho da rede. A necessidade de isolamento do tráfego das redes sem fios poderá implicar por exemplo à atribuição de VLANs para cada SSID definido. A criação de sistemas de colecta de Logs centralizada e sistemas de gestão e monitorização (SIEM) são também fundamentais.

O resultado desta actividade será um documento de **políticas de segurança em redes sem fios** e um **plano de implementação de controlos**. Os controlos identificados materializam-se em actividades, como sejam a implementação de WIDS/WIPS ou segmentação de uma rede em SSIDs e VLANs.

7.4. Implementação de controlos de segurança

Em face do planeamento definido no Plano de Implementação de Controlos na fase anterior, serão desenvolvidas as actividades de projecto identificadas, que contemplarão:

- Desenho de arquitecturas de rede (com e sem fios) e respectiva implementação;
- Desenho das especificações de sistemas, protocolos e mecanismos de segurança a implementar (soluções de autenticação, protocolos de cifra, etc);
- Desenho e implementação de processos de gestão de utilizadores e perfis de acesso;
- Desenho e implementação de processos de gestão de alterações às configurações de segurança em redes, e dispositivos de acesso;
- Desenho e implementação de processos de gestão de controlo e monitorização (sistemas de detecção de intrusão e prevenção (WIDS/WIPS);
- Desenho e implementação de processos de gestão de incidentes de segurança.

Se numa primeira iteração do processo de implementação de controlos de uma rede sem fios forem implementadas as actividades sumariamente descritas anteriormente, ou outras consideradas necessárias para a implementação dos controlos obtidos da análise de risco, em futuras iterações, o esforço a desenvolver será normalmente inferior.

O resultado desta fase do processo será o desenvolvimento de um projecto que contemple as diversas actividades de implementação de controlos.

7.5. Monitorização, revisão e melhoria

A gestão de segurança é um processo contínuo que necessita de indicadores para desenvolver actividades de melhoria. A avaliação regular das plataformas e processos permite assegurar a melhoria de qualidade dos mesmos e responder de forma mais eficaz e eficiente às mudanças organizacionais ou tecnológicas. A identificação de oportunidades face a novas normas de segurança ou de novas tecnologias de rede (como seja 802.11ac) poderá ajudar a organização a endereçar novas necessidades (ex: BYOD, *cloud computing*, Internet das coisas - IoT).
Neste domínio propõe-se uma abordagem segregada em três vectores - Monitorização, Revisão e Melhoria -, cujo resultado será um conjunto de propostas de alteração a serem incorporadas no próximo ciclo do processo.

7.5.1. Monitorização

Em resultado do plano de implementação, fica disponível um conjunto de mecanismos e infra-estruturas que permitem uma monitorização contínua a processos e infra-estruturas. Desta forma deveremos garantir o acompanhamento contínuo nos seguintes aspectos:

- Gestão das iniciativas do plano de implementação
    - Monitorar o estado actual dos projectos e resolver conflitos de recursos
    - Monitorização de implementação dos controlos
- Serviços de Operação
    - Monitorar níveis de serviço
    - Gestão de incidentes de segurança
        - Detecção de actividades anómalas em redes e sistemas
        - Detecção de tentativa ou acessos não autorizados
- Serviços de auditoria
    - Testes de penetração periódicos
        - Encontrar vulnerabilidades
        - Validar conformidade
    - Análise de vulnerabilidades
        - Para encontrar novas vulnerabilidades
        - Encontrar sistemas desactualizados ou com segurança fraca
    - Identificação de Rouge APs
    - Monitorizar actividade através de WIDS/WIPS

7.5.2. Revisão

O processo de revisão visa garantir que os controlos e políticas definidas se encontram devidamente implementadas. Como resultado poderemos obter um conjunto de "não conformidades" que servirão de *input* a um novo ciclo do processo, para promover o seu tratamento.

As actividades envolvidas deverão ser efectuadas com sazonalidade e deverão endereçar os seguintes aspectos:

- Revisão de processos
    - Gestão de autorização de acesso
    - Gestão de incidentes de segurança
- Revisão de controlos
    - Configuração de segurança dos dispositivos móveis
    - Configuração de segurança dos equipamentos de rede
    - Configuração de segurança nos recursos, sistemas e aplicações
    - Revisão dos perfis dos utilizadores
    - Revisão dos acessos autorizados
- Revisão de requisitos
    - Revisão da criticidade da informação e dos recursos disponibilizados
    - Revisão dos requisitos de utilizadores versus controlos implementados (*Gap Analysis*)

7.5.3. Melhoria

Em face da informação recolhida nos processos de monitorização e de revisão, bem como de alterações que ocorram devido a aspectos legais, concorrenciais, metodologias de avaliação de risco, critérios de impacto ou novas tecnologias (BYOD, 802.11ac, 802.11i), torna-se necessário identificar propostas de melhoria que mantenham ou melhorem a eficiência e eficácia dos controlos de segurança.

A proposta de metodologia para a segurança de redes sem fios baseada em análise de riscos permite:

- Identificar modelos de arquitectura e segurança que suportem as necessidades de mobilidade, desempenho e da qualidade de serviço tendo em vista a sua utilização em ambientes empresariais;
- Propor um modelo de suporte a tomadas de decisão relativamente à escolha da arquitectura, dos modelos de segurança, ou das tecnologias envolvidas;

8. Conclusões

8.1. Conclusão

A tecnologia de rede sem fios veio possibilitar a realização do conceito de mobilidade no acesso à informação. As pessoas já estão habituadas à mobilidade nas aplicações de voz devido à massificação de telemóveis, mas com o grande crescimento de utilização de dispositivos moveis, computadores portáteis, *smartphones* e *tablets*, e com a disponibilidade de redes sem fios em espaços públicos (como empresas ou universidades), reduziu-se a dificuldade e complexidade de acesso e utilização das redes sem fios. As empresas olham este movimento tecnológico com muito interesse pois permite reduzir investimentos estruturais, quer em termos de instalação de redes como de facilidade de utilização de recursos locais ou na nuvem.

Os aspectos de segurança têm sido um obstáculo psicológico na adopção da tecnologia de rede sem fios, mas com a metodologia que se propôs nesta dissertação para um processo de desenho, implementação e operação das redes sem fios, poder-se-á assegurar aos gestores e implementadores uma *framework* que identifica as melhores práticas e mecanismos de segurança no desenho da rede sem fios para assegurar a melhor protecção dos activos da organização.

8.2. Trabalho futuro

A publicação da norma IEEE 802.11ac vem possibilitar a utilização de uma rede sem fios de alto débito até 6,93 Gbps, permitindo a sua utilização por múltiplos dispositivos com requisitos da largura de banda e latência elevados e permitindo praticamente adoptar esta tecnologia por defeito no desenho de novas redes.

Como actividades futuras propõe-se:

- O estudo de como endereçar a monitorização de maiores intervalos de frequências para serem monitorizados para a detecção de Rouge AP;
- Qual o impacto que o aumento da velocidade da rede poderá provocar ao permitir que trafego malicioso possa ser injectado mais rapidamente na rede.
- Identificar e analisar fragilidades que possam existir no protocolo IEEE 802.11ac;
- Análise do impacto numa organização que queira implementar este novo protocolo, face a um processo de coexistência com protocolos anteriores (IEEE 801.11g, IEEE 802.11n);
- Estudos do impacto nos mecanismos de monitorização e detecção de ataques

- Análise do impacto da utilização crescente de dispositivos nas redes sem fios como sejam os fenómenos BYOD (*Bring Your Own Device*) e IoT (*Internet of Things*),

Bibliografia

[1] Cisco, “Cisco Visual Networking Index: Forecast and Methodology, 2011-2016,” Cisco, 2012.

[2] IEEE, “OFFICIAL IEEE 802.11 WORKING GROUP PROJECT TIMELINES,” IEEE, 22 03 2013. [Online]. Available: http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm. [Acedido em 30 03 2013].

[3] Cisco, “Enterprise Networks and the Drive for IPv6,” 20 03 2013. [Online]. Available: http://blogs.cisco.com/wireless/enterprise-networks-and-the-drive-for-ipv6/. [Acedido em 01 09 2014].

[4] M. S. Gast, 802.11n: A survival Guide, O'Reilly, 2012.

[5] A. Defense, “Wireless LAN Security – What Hackers Know That You Don’t,” 2005. [Online]. Available: http://www.airdefense.net/whitepapers/downloads/what_hackers.pdf. [Acedido em 24 Maio 2014].

[6] K. Fleming, “Wireless Security Initiatives,” Maio 2005. [Online]. Available: http://telecom.gmu.edu/publications/Kieth-Fleming-Wireless-Security-Project-f2-May-2005.doc. [Acedido em Março 2014].

[7] ISO, “ISO 27005 - Information technology – Security techniques – Information security risk management,” ISO, 2011.

[8] W. Stallings, Cryptography and Network Security - Principles and Practices, 3nd ed., Prentice Hall, 2003.

[9] A. S. Eli Bidham, Differencial Cryptanalysis of Data Encription Standard, Springer Verlag, 1993.

[10] A. S. Eli Biham, Differential cryptanalysis of full 16-round DES, Advances in Cryptology, Springer Verlag, 1993.

[11] M. Matsui, The First Experimental Cryptanalysis of the Data Encription Standard, CRYPTO, 1994.

[12] B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, 2nd ed., John Wiley & Sons, Inc, 1996.

[13] N. F. P. 197, Advanced Encryption Standard, 2001.

[14] H. A. D. (. M. S. Shraddha Soni, Analysis and Comparison between AES and DES Cryptographic Algorithm, Vols. %1 de %2Volume 2, Issue 6, International Journal of Engineering and Innovative Technology (IJEIT), Dezembro 2012.

[15] F. (. I. P. S. P. 81, National Bureau Standards - DES Modes of Operation, Department of Commerce, 1980.

[16] I. M. A. S. S. Fluhrer, Weakness in the key Scheduling Algoritm of RC4, 2001.

[17] W. D. e. M. Hellman, New Directions in Cryptography, AFIPS Natioonal Computer Conference, 1976.

[18] S. A. e. A. L. Rivest R, “A Method for Obtaining Digital Signatures and Public Key Cryptosystems,” em *Communications of the ACM*, 1978.

[19] NSA, Secure Hash Standard - NIST FIPS PUB 180-1, NIST, 1995.

[20] NSA, Secure Hash Algorithm - NIST FIPS PUB 180-2, NIST, 2002.

[21] R. Rivest, RFC 1320 - The MD5 Message-Digest Algorithm, IETF, 1992.

[22] B. Schneier, “Cryptanalysis of SHA-1,” 2005. [Online]. Available: https://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html. [Acedido em Março 2014].

[23] D. F. X. L. H. Y. Xiaoyun Wang, “Collision for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD,” Cryptology ePrint, Report 2004/199, 2013.

[24] W. D. e. M. Hellman, “New Directions in Cryptography,” IEEE Trans. On Information Theory, Novembro 1976.

[25] S. a. M.E.Hrllman, “An Improved Algorithm for Computing Logarithms in GF(p) and its Cryptographic Significance,” IEEE Trans. on Information Theory, 1978.

[26] T. D. a. C. Allen, “The TLS Protocol Version 1.0 - RFC 2246,” IETF, 1999.

[27] S. a. R. Atkinson, “Security Architecture for the Internet Protocol. RFC 2401,” IETF, 1998.

[28] IETF, “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification,” Janeiro 2010. [Online]. Available: http://tools.ietf.org/html/rfc5751. [Acedido em 31 Maio 2014].

[29] http://www.verisign.com/, “SSL Certificates from Symantec Powered by VeriSign,” Symantec, 2014. [Online]. Available: http://www.verisign.com/. [Acedido em 01 Junho 2014].

[30] DigiCert, “DigiCert - SSL Digital Certificate Authority,” DigiCert, 2014. [Online]. Available: http://www.digicert.com/. [Acedido em 01 Junho 2014].

[31] Geotrust, “Geotrust - SSL Certificates, Web Security and Signing Products,” Geotrust, 2014. [Online]. Available: https://www.geotrust.com/. [Acedido em 01 Junho 2014].

[32] W. W. a. D. R.Housley, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile - RFC 3280,” IETF, 2002.

[33] ITU-T, “Itu-t recommendation x.509 (1997 e), Information Technology - Open Systems Interconnection - The directory:Authentication Framework,” ITU-T, 1997.

[34] S. W. L. A. R. M. a. W. S. D. C. Rigney, “RFC 2865 Remote Authentication Dial In User Service (RADIUS)”,” Junho 2000. [Online]. Available: http://tools.ietf.org/pdf/rfc2865.pdf. [Acedido em Novembro 2013].

[35] E. J. A. J. L. G. Z. E. V. Fajardo, “Diameter Base Protocol,” IETF, 2012. [Online]. Available: http://tools.ietf.org/html/rfc6733. [Acedido em Novembro 2013].

[36] A. K. E. J. Walker, “Common Open Policy Service (COPS) Over Transport Layer Security (TLS),” Dezembro 2005. [Online]. Available: http://tools.ietf.org/html/rfc4261.

[37] I. 802.11-04/0123r1, “802.11i Overview,” Fevereiro 2005. [Online]. Available: http://grouper.ieee.org/groups/802/16/liaison/docs/80211-05_0123r1.pdf. [Acedido em Março 2014].

[38] I. P. A. P. Congdon., “IEEE 802.1x Overview. Port Based Network Access Control,” Março 2000. [Online]. Available: http://www.ieee802.org/1/files/public/docs2000/P8021XOverview.PDF. [Acedido em Fevereiro 2014].

[39] B. A. a. T. M. D. Simon, “IEEE Security and 802.1x,” Março 2000. [Online]. Available: http://www.ieee802.org/1/files/public/docs2000/8021xSecurity.PDF. [Acedido em Março 2014].

[40] S. S. A. B. D. M. K. Sankar, Cisco Wireless LAN Security, Cisco Press, 2005.

[41] N. S. a. Y. C. J. W. W. A. Arbaugh, “Your 802.11 Wireless Network has No Clothes,” Março 2001. [Online]. Available: http://www.cs.umd.edu/~waa/wireless.pdf. [Acedido em 01 Junho 2014].

[42] I. G. a. D. W. N. Borisov, “Intercepting Mobile Communications – The insecurity of 802.11,” Julho 2001. [Online]. Available: http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf. [Acedido em 2014 Junho 2014].

[43] I. M. a. A. S. S. Fluhrer, “Weaknesses in the Key Scheduling Algorithm of RC4,” Agosto 2001. [Online]. Available: http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf. [Acedido em 24 Maio 2014].

[44] Greenpacket, "Wi-Fi FOR A CONNECTED WORLD TOWARDS NEXT GENERATION NETWORKS," 2012.

[45] Wireless Broadband Alliance, “WBA Industry Report 2011, Global Developments in Public WiFi,” 2012.

[46] Wireless Broadband Alliance, “WBA Industry Report 2012, Global Trends in Public WiFi - Next-Generation Hotspot: Moving from Standardization to Commercialization,” 2012.